UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Introducción al álgebra conmutativa

Autor/es

SANTIAGO CEBELLAN MARTINEZ

Director/es

JESÚS ANTONIO LALIENA CLEMENTE

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2019-20

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

Introducción al álgebra conmutativa

Realizado por:

Santiago Cebellán Martínez

Tutelado por:

Jesús Antonio Laliena Clemente

Logroño, Junio, 2020

Índice

Resumen

En este trabajo estudiaremos los fundamentos básicos de la geometría algebraica clásica tales como los conjuntos afines algebraicos, las variedades afines o el teorema de ceros de Hilbert. Además para que estos conceptos se puedan entender necesitaremos explicar bastantes conceptos de álgebra conmutativa tales como anillos noetherianos, radicales, enteros algebraicos o localización. Finalmente, para completar el trabajo daremos una breve introducción a la generalización de la geometría algebraica sobre anillos conmutativos cualquiera.

Abstract

In this thesis we will study the fundamentals of classic algebraic geometry such as affine algebraic sets, affine varieties and the Hilbert's Nullstellensatz. In order to understand all those concepts we will need to also introduce plenty of concepts and results belonging to commutative algebra such as noetherian rings, radicals, integral extensions and localization. Finally, to round up the thesis we shall introduce the generalization of the algebraic geometry concepts we have previously seen so we can apply them to arbitrary commutative rings.

Introducción

La geometría algebraica es una rama del álgebra que se encarga de estudiar las soluciones de sistemas de ecuaciones polinomicas. Está rama no se centra tanto en calcular soluciones particulares para sistemas sino busca estudiar las soluciones y sus propiedades a un nivel más abstracto.

Evidentemente la idea de usar conceptos algebraicos para resolver problemas de carácter geométrico no es algo moderno, se pueden encontrar numerosos ejemplos a lo largo de toda la historia. Sin embargo no fue hasta finales del siglo XIX con el desarrollo de las geometrías no euclídeas y las integrales abelianas que empezó a haber un mayor interés en estudiar la geometría y el álgebra de manera conjunta.

A principios del siglo XX cuando a B. L. van der Waerden, Oscar Zariski y André Weil establecieron unos fundamentos estándar para la geometría algebraica. Estos fundamentos estaban basados en conceptos del álgebra conmutativa que estaba empezando a ser desarrollada por aquel entonces. Durante la época anterior la geometría algebraica se limitaba al estudio de anillos de polinomios y conjuntos de ceros para estos polinomios. El enfoque de estos tres matemáticos es el que discutiremos durante la mayor parte de este trabajo.

A mediados del siglo XX Jean Pierre-Serre y Alexander Grothendieck reconstruyeron estos fundamentos para que los conceptos anteriores se pudiesen aplicar a anillos conmutativos R cualquiera.

A día de hoy la geometría algebraica es una de las áreas de las matemáticas más importantes. Está conectada con multitud de campos como por ejemplo el análisis complejo o la topología. Además tiene multitud de aplicaciones ya sea en estadística, en robótica o en teoría de cuerdas [3][4][5].

El objetivo de este trabajo es el estudio de esos primeros resultados de geometría algebraica que relacionan elementos de anillos de polinomios sobre cuerpos con sus soluciones dentro de espacios afines. Estos resultados requieren introducir muchos conceptos del álgebra conmutativa que también estudiaremos.

El trabajo estará estructurado en cinco capítulos. En el primero definiremos los conceptos más básicos en la geometría algebraica clásica, los conjuntos algebraicos afines y sus asociado geométricos los anillos de coordenadas. Además veremos las relaciones fundamentales que existen entre ambos conceptos. Después, en el segundo capítulo estudiaremos la estructura que dichos conjuntos y como se pueden descomponer. Para el tercer capítulo nos centraremos exclusivamente en explicar el teorema de ceros de Hilbert, un importante resultado que nos permite elaborar un diccionario que relaciona conceptos algebraicos y geométricos. El cuarto capítulo consistirá principalmente en estudiar la técnica algebraica conocida como localización, que posteriormente utilizaremos para definir el cuerpo de funciones racionales sobre un conjunto algebraico afín. Finalmente el quinto y último capítulo cambiará de enfoque y no se centrará en introducir nuevos conceptos sino en generalizar los conceptos anteriores a anillos conmutativos cualesquiera.

El trabajo está basado prácticamente en su totalidad en el libro Abstract Algebra de David S. Dummit y Richard M. Foote [1].

1 Anillos noetherianos y conjuntos algebraicos afines

Por defecto, R denotará un anillo conmutativo con $1 \neq 0$ y k un cuerpo.

Generalmente la estructura de cada capítulo sera la siguiente: empezaremos con resultados y conceptos algebraicos más generales y después los aplicaremos al caso concreto de la geometría algebraica.

Definición. Un anillo conmutativo R es **noetheriano** si satisface la condición de ideales ascendentes: no existe ninguna cadena ascendente infinita de ideales de R. Es decir, para toda cadena ascendente de ideales de R, $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$, existe un entero m tal que $I_k = I_m$ para todo $k \geq m$

Recordemos que un ideal I de un anillo R es un subgrupo abeliano de $(R, +)$ que cumple que $rx \in I$ para todo $r \in R$, $x \in I$.

Proposición 1. Si I es un ideal dentro de un anillo noetheriano R, entonces el cociente R/I es un anillo noetheriano. Cualquier imagen por homomorfismo de un anillo noetheriano es noetheriano (un homorfismo de anillos es una aplicación $f\colon R \to S$ de modo que $f(x+y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$ para cada $x, y \in R$).

Demostración:

La primera afirmación sale directamente del cuarto teorema de isomorfia. La segunda de la primera más el primer teorema de isomorfia. Ver anexo sobre teoría de modulos al final del trabajo. ■

Teorema 2. Las siguientes afirmaciones son equivalentes:

1. R es un anillo noetheriano.
2. Todo conjunto no vacío de ideales de R contiene un elemento maximal bajo la inclusión ($\subseteq$).
3. Todo ideal de R está finitamente generado (es decir, los elementos del ideal son de la forma $r_1 s_1 + \cdots + r_n s_n$ para $r_1, \ldots, r_n$ elementos cualesquiera de R).

Demostración:

$1 \to 2$. Suponemos que hay un conjunto no vacío S de ideales de R sin elemento maximal. Cogiendo un ideal cualquiera en S, I_0, como no es maximal existe I_1 tal que $I_0 \subset I_1$ y a su vez I_1 no es maximal. Procediendo de esta manera podemos encontrar una cadena ascendente infinita de ideales de R, llegando a una contradicción.

$2 \to 3$. Sea I un ideal cualquiera de R y cojamos S el conjunto de todos los ideales finitamente generados contenidos en I. $(0) \in S$ luego $S \neq \emptyset$, entonces por 2) sabemos que S tendrá un elemento maximal. Sea I' dicho elemento maximal. Supongamos que $I' \subsetneq I$, en ese caso existiría $x \in I - I'$. Como asumimos que I' está finitamente generado entonces $I'' = (x) + I'$ ((x) denota aquí el ideal generado por x en R, $\{rx \,|\, r \in R\}$ sería también un ideal finitamente generado contenido en I lo cual contradice que I' sea elemento maximal de S. Por tanto $I = I' \in S$, luego I está finitamente generado.

$3 \to 1$. Sean $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ una cadena ascendente de ideales de R. Sea

$$I = \bigcup_{i=0}^{\infty} I_i$$

I es un ideal de R. Por 3) sabemos que I está finitamente generado por digamos, $(a_0, a_1, \ldots, a_m)$. Como cada $a_i \in I$ existe un entero positivo n_i tal que $a_i \in I_{n_i}$. Sea $n = max(n_0, \ldots, n_m)$ entonces $a_i \in I_n$ para todo i (porque en cada caso $I_{n_i} \subseteq I_n$), luego $I \subseteq I_n$ y por definición de I evidentemente $I = I_n$. Ahora para todo $k \geq n$ tenemos $I_n \subseteq I_k \subseteq I = I_n$, luego $I_n = I_k$. ■

Teorema 3. (*Teorema de Bases de Hilbert*) Si R es un anillo noetheriano, entonces el anillo de polinomios $R[x]$ también lo es.

Demostración:

Sea I un ideal cualquiera de $R[x]$, vamos a ver que está finitamente generado.

Sea $L \subseteq R$ el conjunto de coeficientes directores de elementos de I. Obviamente $0 \in L$, además si $f = ax^d + \ldots$ y $g = bx^e + \ldots$ son polinomios de I, entonces $a, b \in L$. Cojamos $r \in R$ y comprobemos que $ra - b \in L$, efectivamente el polinomio $rx^e f - x^d g \in I$ y $ra - b \in L$ porque es el coeficiente director de dicho polinomio. Esto prueba que L es un ideal en R. Al ser L un ideal en un anillo noetheriano está finitamente generado por digamos, $\{a_1, a_2, \ldots, a_n\}$ con $a_i \in R$. A cada a_i podemos asignarle un polinomio f_i de grado e_i en I del que es coeficiente director. Denotaremos $M = max\{e_1, \ldots, e_n\}$.

Ahora para cada $d = 0, 1, \ldots, M-1$ definimos L_d el conjunto de coeficientes directores de polinomios de I de grado d. Usando argumentos prácticamente idénticos a los del párrafo anterior podemos comprobar que L_d es un ideal de R y por tanto finitamente generado por el conjunto $\{b_{d,1}, \ldots, b_{d,n_d}\}$ con polinomios asociados $\{f_{d,1}, \ldots, f_{d,n_d}\} \subseteq I$.

Ahora comprobaremos que:

$$I' := (\{f_1, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \leq d < M, 1 \leq i \leq n_d\}) = I$$

Que $I' \subseteq I$ ya que todos los elementos que generan I' están en I. Supongamos entonces que $I' \neq I$ y cojamos $f \in I$ de grado mínimo tal que $f \notin I'$, denotaremos por a al coeficiente director de f y como d al grado de f.
Supongamos que $d \geq M$. Como a está en L podemos escribirlo como combinación de los elementos generadores de L, $a = r_1 a_1 + \cdots + r_n a_n$. Usando los polinomios asociados a cada a_i definimos el polinomio $g = r_1 x^{d-e_1} f_1 + \cdots + r_n x^{d-e_n} f_n$ que será un polinomio en I' de grado d y con coeficiente director a, luego $f - g$ tendrá grado estrictamente menor que d. Como f tiene grado mínimo dentro de los polinomios de I que no están en I' necesariamente $f - g = h \in I'$ luego $f = g + h$, y como $g, h \in I'$, $f = g + h \in I'$ lo cual es una contradicción. Por tanto de existir f deberá tener grado estrictamente menor que M.

Supongamos que $d < M$. En este caso repetimos el mismo razonamiento que en el párrafo anterior para L_d en vez de L. Llegaremos a que de existir f no puede tener grado $d < M$.

Por tanto no existe ningún $f \in I$ que no este en I'. Por doble contenido $I = I'$ y I' está finitamente generado. Que todo ideal I de $R[x]$ esté finitamente es equivalente a que $R[x]$ sea noetheriano como queríamos probar. ■

Ejemplo:

Todos cuerpo k es un anillo noetheriano porque solo contiene dos ideales (0) y k.

Corolario 4. El anillo de polinomios $k[x_1, x_2, \ldots, x_n]$ con coeficientes tomados de un cuerpo k es un anillo noetheriano.

Definición. Sea k un cuerpo. Un anillo R es una **k-álgebra** si k (o una copia isomorfica de k) está contenido en el centro de R (el conjunto de elementos de R que conmutan con todos los demás) y la identidad de k coincide con la identidad de R. Además:

1. El anillo R es una k-álgebra finitamente generada si es generada como anillo por k junto a una cantidad finita de elementos de R.
2. Sean R y S k-algebras. Una aplicación $\psi : R \longrightarrow S$ es un **homomorfismo de k-algebras** si ψ es un homomorfismo de anillos que es la identidad para los elementos de k.

Corolario 5. El anillo R es un k-álgebra finitamente generada si y solo si existe un homomorfismo de k-álgebras:

$$\phi : k[x_1, x_2, \ldots, x_n] \to R$$

desde el anillo de polinomios sobre k con un numero finito de variables a R. Como consecuencia todo k-álgebra finitamente generada sobre un cuerpo k es Noetheriana.

Ejemplos:

Los anillos de polinomios en una o más variables sobre un cuerpo k son k-álgebras, los elementos de k pueden verse como los polinomios constantes. Además si I es un ideal propio en $k[x_1, \ldots, x_n]$ entonces $k[x_1, \ldots, x_n]/I$ también será una k-álgebra.

1.1 Conjuntos algebraicos afines

La idea principal detrás de la "geometría algebraica" es relacionar conceptos geométricos con conceptos algebraicos como ideales. Nosotros empezaremos centrándonos en anillos del tipo $k[x_1, \ldots, x_n]$. La ventaja de estos anillos es que al ser noetherianos muchas cuestiones sobre ideales se vuelven mucho más sencillas de estudiar.

Primero un poco de notación:

Usaremos $\mathbb{A}^n$ para referirnos al conjunto de n-tuplas sobre un cuerpo k y llamaremos a este conjunto n-espacio afin sobre k. Si $x_1, x_2, \ldots, x_n$ son variables independientes sobre k, los elementos de $k[x_1, x_2, \ldots, x_n]$ pueden ser vistos como funciones $f : \mathbb{A}^n \to k$:

$$f : (a_1, a_2, \ldots, a_n) \to f(a_1, a_2, \ldots, a_n)$$

Viendo los polinomios de esta manera podemos expresar $k[x_1, x_2, \ldots, x_n]$ como $k[\mathbb{A}^n]$ y llamarlo *anillo de coordenadas de* $\mathbb{A}^n$.

Para cada subconjunto S de $k[\mathbb{A}^n]$ podemos definir un subconjunto de $\mathbb{A}^n$, $\mathcal{Z}(S)$, dado por todos los puntos de $\mathbb{A}^n$ en los que todos los elementos de S se anulan simultáneamente.

$$\mathcal{Z}(S) := \{(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n | f(a_1, a_2, \ldots, a_n) = 0 \quad \forall f \in S\}$$

Además, por convenio $\mathcal{Z}(\emptyset) = \mathbb{A}^n$.

Definición. Decimos que un subconjunto V de $\mathbb{A}$ es un **conjunto algebraico afín** (o sencillamente conjunto algebraico) si $V = \mathcal{Z}(S)$ para algún $S \subseteq k[\mathbb{A}^n]$.

En el caso de que $S = \{f\}$ o $S = \{f_1, f_2, \ldots, f_n\}$ escribiremos simplemente $\mathcal{Z}(f)$ o $\mathcal{Z}(f_1, f_2, \ldots, f_n)$ y diremos que se trata del lugar geométrico de $f_1, f_2, \ldots, f_n$.

Ejemplos:

1. Si $k = \mathbb{R}$, $n = 1$ tenemos $\mathbb{A}^1 = \mathbb{R}$ y $k[\mathbb{A}^1] = \mathbb{R}[x]$. Elegimos $S = \{x^2\} \in k[\mathbb{A}^1]$, en este caso $\mathcal{Z}(S)$ (o $\mathcal{Z}(x^2)$) es sencillamente el conjunto unipuntual $\{0\}$.
2. Todo punto único $(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ forma su propio conjunto algebraico como $\mathcal{Z}(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$.

Los conjuntos algebraicos afines nos dan una relación natural entre el espacio afín $\mathbb{A}^n$ y el anillo $k[\mathbb{A}^n]$. Es el concepto más fundamental para este trabajo, luego es interesante dar algunas propiedades sobre la aplicación $\mathcal{Z}$ que los define.

Proposición 6. Con la notación que hemos estado usando hasta ahora, sean S y T subconjuntos de $k[\mathbb{A}^n]$.

1. Si $S \subseteq T$ entonces $\mathcal{Z}(T) \subseteq \mathcal{Z}(S)$ ($\mathcal{Z}$ invierte la inclusión).
2. $\mathcal{Z}(S) = \mathcal{Z}(I)$, donde $I = (S)$ el ideal generado a partir de S.
3. La intersección arbitraria de conjuntos algebraicos afines es un conjunto algebraico afín. Más concretamente, si $\{S_j\}$ en colección de subconjuntos cualesquiera de $k[\mathbb{A}^n]$, entonces:
$$\cap \mathcal{Z}(S_j) = \mathcal{Z}(\cup S_j)$$
4. La unión de dos conjuntos algebraicos afines es a su vez un conjunto algebraico afín. Más concretamente, $\mathcal{Z}(S) \cup \mathcal{Z}(T) = \mathcal{Z}(IJ)$, siendo I, J ideales en $k[\mathbb{A}^n]$ y IJ su producto.
5. $\mathcal{Z}(0) = \mathbb{A}^n$ y $\mathcal{Z}(1) = \emptyset$ (0 y 1 funciones constantes).

Algunas observaciones:

- De las propiedades $(3), (4), (5)$ vemos que los conjuntos algebraicos tienen las propiedades para ser los cerrados de una topología (generalizar (4) a uniones finitas es fácil, basta notar que la unión es asociativa).
- Por la propiedad (2) vemos que podemos concretar la definición de conjunto algebraico afín de:
$$V = \mathcal{Z}(S) \text{ para } S \text{ algún subconjunto de } k[\mathbb{A}^n]$$
a
$$V = \mathcal{Z}(I) \text{ para } I \text{ algún ideal de } k[\mathbb{A}^n]$$
sin perdida de generalidad.

- El ideal (o subconjunto) de $k[\mathbb{A}^n]$ que determina un conjunto algebraico V no tiene por qué ser único.

Hemos visto $\mathcal{Z}$ como una aplicación que nos permitía relacionar $k[\mathbb{A}^n]$ con $\mathbb{A}^n$ a través de sus subconjuntos. De la definición de $\mathcal{Z}$ no cuesta mucho imaginar una aplicación que nos dé una relación "inversa", de $\mathbb{A}^n$ a $k[\mathbb{A}^n]$. Sea $A \subseteq \mathbb{A}^n$ definimos:

$$\mathcal{I}(A) = \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in A\}$$

Es inmediato ver que $\mathcal{I}(A)$ es el mayor ideal para el cual todos sus elementos son simultáneamente cero en A.

$$\mathcal{I} : \{\text{subconjuntos de } \mathbb{A}^n\} \longrightarrow \{\text{ideales de } k[\mathbb{A}^n]\}$$

Ejemplos:

- En el plano $\mathbb{A}^2$ con $k = \mathbb{R}$, $\mathcal{I}$(eje x) es el ideal generado por y en el anillo $\mathbb{R}[x, y]$
- Sobre cualquier cuerpo k, sea $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Denotemos $A = \mathcal{I}(a_1, \ldots, a_n)$. Sea ϕ: $k[x_1, \ldots, x_n] \to k$ la aplicación para la que $\phi(f) = f(a_1, \ldots, a_n)$, ϕ es suprayectiva y tiene núcleo A. Por el primer teorema de isomorfia $k[x_1, \ldots, x_n]/A \cong k$ un cuerpo, luego $A = \mathcal{I}(a_1, \ldots, a_n)$ es un ideal maximal.

  Ahora sea φ: $k[\mathbb{A}^n] \to k[\mathbb{A}^n]$ tal que $\varphi(f(x_1, \ldots, x_n)) = f(x_1+a_1, \ldots, x_n+a_n)$ y sea ψ: $k[\mathbb{A}^n] \to k$ que evalúa los polinomios en 0. Es fácil ver que $\phi = \psi \circ \varphi$, que $ker\, \psi = (x_1, \ldots, x_n)$ y que $\varphi^-1((x_1, \ldots, x_n)) = (x_1 - a_1, \ldots, x_n - a_n)$. Por tanto $ker\, \phi = A = (x_1 - a_1, \ldots, x_n - a_n)$.

$$\mathcal{I}(a_1, a_2, \ldots, a_n) = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$$

La aplicación $\mathcal{I}$ es el análogo a $\mathcal{Z}$ dentro del anillo $k[\mathbb{A}^n]$ y veremos que ambas están intrínsecamente relacionadas. Por ahora empecemos dando algunas propiedades fundamentales.

Proposición 7. Siguiendo la notación como hasta ahora, sean A y B subconjuntos de $\mathbb{A}^n$

1. Si $A \subseteq B$ entonces $\mathcal{I}(B) \subseteq \mathcal{I}(A)$ ($\mathcal{I}$ invierte la inclusión)
2. $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$.
3. $\mathcal{I}(\emptyset) = k[x_1, x_2, \ldots, x_n]$ y, si k es infinito, $\mathcal{I}(\mathbb{A}^n) = 0$

Tan importante como $\mathcal{Z}$ o $\mathcal{I}$ son las relaciones que se establecen entre ellas.

Proposición 8. Siguiendo la notación anterior.

1. Si A es un subconjunto de $\mathbb{A}^n$ entonces $A \subseteq \mathcal{Z}(\mathcal{I}(A))$ y si I es un ideal de $k[\mathbb{A}^n]$ entonces, $I \subseteq \mathcal{I}(\mathcal{Z}(I))$

2. Si $V = \mathcal{I}(I)$ un conjunto algebraico afín entonces $V = \mathcal{Z}(\mathcal{I}(V))$, y si $I = \mathcal{I}(A)$ entonces $\mathcal{I}(\mathcal{Z}(I)) = I$.

El último inciso nos dice que si nos limitamos a evaluar en los conjuntos algebraicos afines y en los ideales en $k[\mathbb{A}^n]$ de la forma $I = \mathcal{Z}(V)$ entonces las aplicaciones $\mathcal{Z}$ y $\mathcal{I}$ actúan como inversa una de la otra. Esto lo usaremos más adelante para establecer biyecciones entre subconjuntos de $\mathbb{A}^n$ y $k[\mathbb{A}^n]$.

Definición. Si $V \subseteq \mathbb{A}^n$ es un conjunto algebraico afín, entonces el anillo cociente $k[\mathbb{A}^n]/\mathcal{I}(V)$ es el **anillo de coordenadas de** V y se denota $k[V]$.

Sean f y g funciones de $k[\mathbb{A}^n]$ entonces $f \sim g$ en $k[V]$ si y solo si $f - g \in \mathcal{I}(V)$ por definición de $\mathcal{I}(V)$, si y solo si $f - g = 0$ en todo V es decir, si y solo si f y g definen la misma función cuando se restringen a V. Podemos ver $k[V]$ como todas las funciones distintas que surgen de restringir funciones de $k[\mathbb{A}^n]$ a ser evaluadas en V.

Como $k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$ está generado como k-álgebra por $x_1, \ldots, x_n$. Entonces claramente $k[V]$ está generada como k-álgebra por $\overline{x}_1, \ldots, \overline{x}_n$ luego es una k-álgebra finitamente generada.

A partir de aquí usaremos V para referirnos a un conjunto algebraico afín en $\mathbb{A}^n$ y W para referirnos a un conjunto algebraico afín en $\mathbb{A}^m$, ambos sobre el mismo cuerpo k.

Definición. Una aplicación $\varphi : V \to W$ recibe el nombre de **morfismo** entre conjuntos algebraicos si existen polinomios $\varphi_1, \varphi_2, \ldots, \varphi_m \in k[x_1, x_2, \ldots, x_n]$ de tal forma que:

$$\varphi((a_1, \ldots, a_n)) = (\varphi_1(a_1, \ldots, a_n), \ldots, \varphi_m(a_1, \ldots, a_n)) \quad \forall (a_1, \ldots, a_n) \in V$$

El morfismo $\varphi : V \to W$ es un **isomorfismo** si existe un morfismo inverso $\psi : W \to V$ tal que $\varphi \circ \psi = 1_W$ y $\psi \circ \varphi = 1_V$.

En general $\varphi_1, \varphi_2, \ldots, \varphi_m$ no tienen por qué ser únicos.

Sea F un polinomio en $k[\mathbb{A}^m]$ y $\varphi : V \to W$ un morfismo, entonces $F \circ \varphi = F(\varphi_1, \ldots, \varphi_m)$ es un polinomio en $k[\mathbb{A}^n]$. Si $F \in \mathcal{I}(W)$ como $\varphi(a_1, \ldots, a_n) \in W$ para todo $(a_1, \ldots, a_n) \in V$ entonces $F \circ \varphi \in \mathcal{I}(V)$. Entonces la aplicación inducida por φ:

$$\begin{array}{rccc} \widetilde{\varphi}\colon & k[W] & \to & k[V] \\ & f & \to & f \circ \varphi \end{array}$$

Está bien definida. Además no es difícil comprobar que se trata de un homomorfismo de k-álgebras. Establecemos esto y más en el siguiente teorema.

Teorema 9. Sea $V \subseteq \mathbb{A}^n$ y $W \subseteq \mathbb{A}^m$ conjuntos algebraicos afines sobre un cuerpo k. Entonces hay una correspondencia biyectiva:

Morfismos de V a W como conjuntos algebraicos	$\longrightarrow$ $\longleftarrow$	Homomorfismos de k-algebras de $k[W]$ a $k[V]$

Con más detalle:

1. Todo morfismo $\varphi\colon V \to W$ induce un homomorfismo de k-álgebras asociado $\widetilde{\varphi}\colon k[W] \to k[V]$ definido por $\widetilde{\varphi}(f) = f \circ \varphi$.

2. Todo homomorfismo de k-álgebras $\phi\colon k[W] \to k[V]$ es inducido por un único morfismo $\varphi\colon V \to W$ tal que $\phi = \widetilde{\varphi}$.

3. Si $\varphi\colon V \to W$ y $\psi\colon W \to U$ son morfismos entre conjuntos algebraicos afines, entonces $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}\colon k[U] \to k[V]$

4. El morfismo $\varphi\colon V \to W$ es un isomorfismo si y solo si $\widetilde{\varphi}\colon k[W] \to k[V]$ es un isomorfismo de k-álgebras.

Demostración:

1. *Comprobemos que efectivamente $\widetilde{\varphi}$ es un homomorfismo de k-álgebras:*

   - *Bien definida: ya lo hemos visto.*
   - *Respeta la suma:* $\widetilde{\varphi}(f+g) = (f+g)\circ\varphi = f\circ\varphi + g\circ\varphi = \widetilde{\varphi}(f) + \widetilde{\varphi}(g)$.
   - *Respecta el producto:* $\widetilde{\varphi}(fg) = fg\circ\varphi = (f\circ\varphi)(g\circ\varphi) = \widetilde{\varphi}(f)\widetilde{\varphi}(g)$.
   - *Es la identidad para k: $a \in k$ polinomio constante,* $\widetilde{\varphi}(a) = a\circ\varphi = a(\varphi_1, \ldots, \varphi_m) = a$.

2. *Supongamos que ϕ es un homomorfismo de k-álgebras de $k[W] = k[x_1, \ldots, x_m]/\mathcal{I}(W)$ a $k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$. Sean F_i representantes en $k[x_1, \ldots, x_m]$ de las imágenes bajo ϕ de $\overline{x}_i \in k[W]$ (la clase de equivalencia de x_i en $k[W]$). Definimos ahora $\varphi = (F_1, \ldots, F_m)$ aplicación de polinomios de $\mathbb{A}^n$ a $\mathbb{A}^m$. Si vemos que $\varphi(V) \subseteq W$ tendremos que la restricción $\varphi\colon V \to W$ es un morfismo.*
Cojamos $g \in \mathcal{I}(W)$. Teniendo en cuenta que $k[W]$ es una k-álgebra finitamente generada por $\overline{x}_1, \ldots, \overline{x}_m = x_1 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W)$, entonces

$$g = a_0 x_1^{e_{0,1}} \cdots x_m^{e_{0,m}} + \ldots$$

luego

$$\begin{aligned} g(x_1, \ldots, x_m) + \mathcal{I}(W) = \overline{g} = a_0 \overline{x_1}^{e_{0,1}} \cdots \overline{x_m}^{e_{0,m}} + \ldots = \\ a_0 (x_1^{e_{0,1}} + \mathcal{I}(W)) \cdots (x_m^{e_{0,m}} + \mathcal{I}(W)) + \ldots = \\ g(x_1 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W)) \end{aligned}$$

Por tanto:

$$g(x_1 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W)) = g(x_1, \ldots, x_m) + \mathcal{I}(W) = \mathcal{I}(W) = 0 \in K[W],$$

luego

$$\phi(g(x_1 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W))) = 0 \in k[W],$$

y como ϕ es un homomorfismo de k-álgebras, siguiendo el mismo razonamiento que antes:

$$g(\phi(x_1 + \mathcal{I}(W)), \ldots, x_m + \mathcal{I}(W))) = 0 \in k[W]$$

Por definición de F_i, $\phi(x_i + \mathcal{I}(W)) = F_i + \mathcal{I}(V)$, sustituimos

$$g(F_1 + \mathcal{I}(V), \ldots, F_m + \mathcal{I}(V)) = 0 \in k[V],$$

o lo que es lo mismo

$$g(F_1, \ldots, F_m) \in \mathcal{I}(V).$$

$g(F_1(a_1,\ldots,a_n),\ldots,F_m(a_1,\ldots,a_n))=0$ para todo $(a_1,\ldots,a_n)\in V$, luego todos los polinomios de $\mathcal{I}(W)$ se anulan en $\varphi(a_1,\ldots,a_n)$. Esto es lo mismo que decir que $\varphi(a_1,\ldots,a_n)\in\mathcal{ZI}(W)=W$ por las propiedades que vimos entre $\mathcal{Z}$ e $\mathcal{I}$ cuando W es conjunto afín. Luego efectivamente $\varphi(V)\subseteq W$ y φ es un morfismo inducido por ϕ. Notemos que φ no depende de la elección de los F_i luego ϕ solo induce un único morfismo de esta manera.

Veamos ahora que $\phi=\widetilde{\varphi}$. Para cada x_i

$$\widetilde{\varphi}(x_i+\mathcal{I}(W))=F_i+\mathcal{I}(V)$$

Luego para todo un conjunto que genera $k[W]$ como k-álgebra $\phi=\varphi$ luego $\phi=\varphi$ para todo $k[W]$.

3. Como la composición de polinomios es un polinomio, la composición de morfismos es un morfismo, entonces por (1), *$\widetilde{\psi\circ\varphi}$ es un homomorfismo de k-álgebras. Ahora para $f\in k[U]$:*

$$\widetilde{\psi\circ\varphi}(f)=f\circ(\psi\circ\varphi)+\mathcal{I}(V)=f(\psi\circ\varphi)+\mathcal{I}(V)=f(\psi(\varphi))+\mathcal{I}(V)$$

$$\widetilde{\varphi}\circ\widetilde{\psi}(f)=\widetilde{\varphi}\circ(f\circ\psi+\mathcal{I}(W))=f\circ\psi\circ\varphi+\mathcal{I}(V)=f(\psi(\varphi))+\mathcal{I}(V)$$

4. Sale directamente de (3). ∎

Corolario 10. Supongamos que $\varphi\colon V\to W$ es una aplicación entre conjuntos algebraicos. Entonces φ es un morfismo si y solo si para cada $f\in k[W]$ la composición $f\circ\varphi$ es un elemento de $k[V]$ (una función evaluada en V que toma valores en k). Cuando φ es un morfismo, $\varphi(v)=w$ con $v\in V$ y $w\in W$ si y solo si $\widetilde{\varphi}^{-1}(\mathcal{I}(\{v\}))=\mathcal{I}(\{w\})$.

1.2 Cálculos en conjuntos algebraicos afines y k-álgebras

Esta parte requiere de algunas definiciones y resultados previos. No entraremos en mucho detalle y veremos lo estrictamente necesario.

1.2.1 El algoritmo general de la división y el teorema de eliminación

Para polinomios en una variable el algoritmo de la división entre dos polinomios f y g funciona dividiendo el coeficiente director de f y g para extraer un resto r de grado menor que f. Aquí encontramos nuestro primer problema, en $k[x]$ es fácil ordenar los monomios y por tanto encontrar el término principal, es el monomio qué tenga mayor grado. En varias variables esto no se puede hacer directamente porque no sabemos que variable determina el mayor grado, necesitamos determinar un orden para los monomios. Necesitaremos un orden con las siguientes propiedades.

Definición. Un **orden monomial** es un buen orden "$\geq$" dentro del conjuntos de monomios que satisface que $mm_1\geq mm_2$ si $m_1\geq m_2$ para monomios cualquiera m,m_1,m_2.

En nuestro caso usaremos un orden monomial que se dice lexicográfico. En $k[x_1,x_2,\ldots,x_n]$ establecemos un orden $x_1>x_2>\cdots>x_n$, entonces para monomios de la forma $Ax_1^{a_1}\cdots x_n^{a_n}$, $m_1\geq m_2$ si el grado de la variable x_1, a_1 es mayor en m_1 que en m_2, y si es igual en ambos monomios pasamos a comprobar en $x_2\ldots$ y así sucesivamente siguiendo el orden $x_1>x_2>\cdots>x_n$.

Definición. Fijado un orden monomial en el anillo de polinomios $k[x_1, \ldots, x_n]$. El **término director** de un polinomio no nulo f en $k[x_1, x_2, \ldots, x_n]$, denotado $LT(f)$, es el término monomial de máximo orden en f y $LT(0) = 0$. Definimos el **multigrado de** f, denotado $\partial(f)$, al multigrado del término director de f (el vector con los grados correspondientes a cada variable $x_1, \ldots, x_n$ en $LT(f)$).

Evidentemente el coeficiente director de un polinomio depende del orden monomial que hayamos elegido.

El algoritmo general de la división

Fijemos un orden monomial en $k[x_1, x_2, \ldots, x_n]$. Supongamos que $g_1, \ldots, g_m$ es un conjunto de polinomios no nulos en $k[x_1, \ldots, x_n]$ que usaremos como divisores y f es un polinomio cualquiera en $k[x_1, \ldots, x_n]$ que usaremos como dividendo. Empezaremos con un conjunto de cocientes $q_1, \ldots, q_m$ y un resto r todos iguales a 0.
Comprobaremos si el término director de f, $LT(f)$, es divisible por el término director de algún $g_i \in g_1, \ldots, g_m$ y procederemos de la siguiente manera:

- En el caso de que $LT(f)$ sea divisible entre $LT(g_i)$, digamos, $LT(f) = a_i LT(g_i)$, sumamos a_i a q_i y reemplazamos f por $f - a_i g_i$ (un polinomio con término principal de orden menor según el orden monomial).
- En el caso de que ningún $LT(g_1), \ldots, LT(g_m)$ divida a $LT(f)$, añadimos el coeficiente director de f al resto r y reemplazamos f por $f - LT(f)$ (un polinomio con término principal de menor orden según el orden monomial)

Reiteramos el proceso hasta que el dividendo es 0. Se cumplirá que:

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

Todo $q_i g_i$ tendrá multigrado menor o igual a f y ningún término no nulo de r es divisible por ninguno de los términos directores $LT(g_1), \ldots, LT(g_m)$.

Ejemplo:

Con orden monomial lexicografico $x > y$ vamos a aplicar el algoritmo general de la división para $f = xy + 2y^3 - 1$ entre $\{f_1 = x - 1, f_2 = y^2\}$. Empezamos definiendo el conjunto de cocientes $\{q_1 = 0, q_2 = 0\}$ y el resto $r = 0$

1. Vemos si $LT(f) = xy$ es divisible entre $LT(f_1) = x$ o $LT(f_2) = y^2$. $LT(f) = xy = yLT(f_1)$. Entonces pasaremos al siguiente paso con $f = f - yL(f_1) = 2y^3 + y - 1$ y $q_1 = y + q_1 = y$.
2. Vemos si $LT(f) = y^3$ es divisible entre $LT(f_1) = x$ o $LT(f_2) = y^2$. $LT(f) = 2yLT(f_2)$. Entonces pasaremos al siguiente paso con $f = f - 2yL(f_1) = y - 1$ y $q_2 = 2y + q_2 = 2y$.
3. Vemos si $LT(f) = y$ es divisible entre $LT(f_1) = x$ o $LT(f_2) = y^2$. No lo es, luego pasaremos al siguiente paso con $r = LT(f) + r = y$ y $f = f - LT(f) = -1$.
4. Vemos si $LT(f) = y$ es divisible entre $LT(f_1) = x$ o $LT(f_2) = y^2$. No lo es, luego pasaremos al siguiente paso con $r = LT(f) + r = y - 1$ y $f = f - LT(f) = 0$.

Como el dividendo es 0 el algoritmo concluye con cocientes $\{y, 2y\}$ y resto $y-1$ tenemos que:

$$f = yf_1 + 2yf_2 + (y-1)$$

Bases de Gröbner

Las bases de Gröbner de un ideal dentro de un anillos de polinomios son conjuntos generadores del ideal que al combinarlos con el algoritmo general de la división tienen propiedades extremadamente útiles. Esto es especialmente cierto para aquellas bases de Gröbner que diremos reducidas.

Definición. Fijado un orden monomial en el anillo de polinomios $k[x_1, \ldots, x_n]$.

- Si I es un ideal en $k[x_1, \ldots, x_n]$, el **ideal de términos directores de** I, denotado $LT(I)$ es el ideal generado por lo términos directores de elementos de I.

$$LT(I) = (LT(f) \,|\, f \in I)$$

- Una **base de Gröbner** del ideal I es un conjunto finito de generadores $\{g_1, \ldots, g_m\}$ de I cuyos términos directores generan el ideal de términos directores de I.

Observemos que $LT(I)$ y las bases de Gröbner de I dependerán del orden monomial elegido. La propiedad más importante de las bases de Gröbner es:

Teorema. Fijemos un orden monomial en $k[x_1, \ldots, x_n]$ y supongamos que $\{g_1, \ldots, g_m\}$ es una base de Gröbner del ideal no nulo I en $k[x_1, \ldots, x_n]$. Si aplicamos el algoritmo de la división general con $f \in k[x_1, \ldots, x_n]$ como dividendo y $g_1, \ldots, g_m$ como divisores obtenemos una manera de expresar f:

$$f = \underbrace{q_1 g_1 + \cdots + q_m g_m}_{f_I} + r$$

con $f_I \in I$ y r no divisible entre ningún término director de $LT(g_1), \ldots, LT(g_m)$. Esta expresión es la única de esta forma para cada f. Además r nos da un representante único para la clase de equivalencia de f en $k[x_1, \ldots, x_n]/I$.

Para hallar las bases de Gröbner de un ideal I contamos con las siguientes herramientas:

Proposición. Fijemos un orden monomial en $k[x_1, \ldots, x_n]$ y sea I un ideal no nulo en $k[x_1, \ldots, x_n]$.

1. Si $g_1, \ldots, g_m$ son elementos de I cuyos terminos directores generan $LT(I)$ entonces $\{g_1, \ldots, g_m\}$ es una base de Gröbner de I.
2. El ideal I tiene alguna base de Gröbner.

Definición. Dado un orden monomial en $R = k[x_1, \ldots, x_n]$. Una base de Gröbner $\{g_1, \ldots, g_m\}$ para un ideal no nulo $I \in R$ se denomina **base de Gröbner reducida** si cumple las siguientes condiciones:

1. Cada g_i es un polinomio mónico.

2. Ningún término de g_i es divisible por un ningún término director de otro elemento de la base de Gröbner $LT(g_j)$, $i \neq j$.

Es fácil ver que a partir de una base de Gröbner podemos obtener una base de Gröbner reducida. Conseguir que los elementos sean mónicos es trivial ya que son polinomios sobre un cuerpo. Para la segunda condición lo que hay que hacer es ir sustituyendo cada elemento de la base por su resto al aplicarle el algoritmo general de la división para todos los demás elementos de la base.

La principal ventaja de trabajar con bases de Gröbner reducidas es que al exigir estas condiciones adicionales se consigue que la base de Gröbner sea única para cada ideal.

Teorema. Fijado un orden monomial para $R = k[x_1, ..., x_n]$. Existe una única base de Gröbner reducida para cada ideal I no nulo de R.

El algoritmo de Buchberger

El algoritmo de Buchberger es un algoritmo para encontrar las bases de Gröbner de un ideal. Se basa en el criterio de Buchberger que explicaremos a continuación.

Sean f_1, f_2 dos polinomios en $k[x_1, \ldots, x_n]$ y M el mínimo común múltiplo entre $LT(f_1)$, $LT(f_2)$ (hecho mónico). Entonces podemos cancelar dichos términos principales haciendo:

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2$$

Proposición 11. *(Criterio de Buchberger)* Sea $R = k[x_1, \ldots, x_n]$, fijamos un orden monomial en R. Sea $I = (g_1, \ldots, g_m)$ un ideal no nulo en R, $G = \{g_1, \ldots, g_m\}$ una base de Gröbner de I si y solo si $S(g_1, g_j) \equiv 0 \; mod \, G$ para $1 \leq i < j \leq m$.

Usando el criterio anterior. Sea $I = (g_1, \ldots, g_m)$ un ideal de $k[x_1, \ldots, x_n]$. Si cada $S(g_i, g_j)$ deja resto 0 al ser dividido por $G = \{g_1, \ldots, g_m\}$ usando el algoritmo general de la división, entonces G es una base de Gröbner de I. En caso contrario $S(g_i, g_j)$ dará un resto r no nulo. Ampliamos G con $g_{m+1} = r$, $G' = \{g_1, \ldots, g_m, g_{m+1}\}$ y volvemos a empezar. Es relativamente fácil ver que este procedimiento nos dara una base de Gröbner de I en un número finito de pasos.

Sea $g_{m+1} := r$ como lo acabamos de definir. Por ser r resto de dividir algún $S(g_i, g_j)$ entre $\{g_1, \ldots, g_m\}$ tendremos que ningún término no nulo de r es divisible entre ningún término principal $LT(g_k)$, por tanto $(LT(g_1), \ldots, LT(g_m)) \subsetneq (LT(g_1), \ldots, LT(g_{m+1}))$ a la vez que $I = (g_1, \ldots, g_m) = (g_1, \ldots, g_m, g_{m+1})$. Supongamos que el algoritmo no acaba en un número finito de pasos. Denotemos como $LT(G_k)$ el ideal $(LT(g_1), \ldots, LT(g_m)$ $, \ldots, LT(g_{m+k}))$ resultante de la k-ésima iteración del algoritmo. Entonces $LT(G_1) \subsetneq LT(G_2) \subsetneq \ldots$ es una cadena ascendente infinita de ideales en $k[x_1, \ldots, x_n]$ que es noetheriano, luego dicha cadena tiene que estabilizarse en algún momento, es decir, existe un entero positivo z para el que $LT(G_i) = LT(G_j)$ si $i, j \geq z$. Esto se contradice con que el algoritmo no acabe en un número finito de pasos. Por tanto el algoritmo de Butchberger acabará en un número finito de pasos.

Ejemplo:

Este ejemplo esta sacado de [2]. Sea el ideal de $\mathbb{R}[x, y]$:

$$I = (g_1 = x^2 + 2xy^2, g_2 = xy + 2y^3 - 1)$$

Fijado el orden monomial lexicografico $x > y$ vamos a usar el algoritmo de Butchberger para calcular una base de Gröbner de I. Empezamos calculando:

$$S(g_1, g_2) = \frac{x^2y}{x^2}g_1 - \frac{x^2y}{xy}g_2 = x$$

Evidentemente x que es su propio resto al ser dividido entre $\{g_1, g_2\}$ luego añadimos $g_3 = x$ y repetimos el proceso:

$$S(g_1, g_2) = x = g_3 \equiv 0$$
$$S(g_2, g_3) = g_2 - yg_1 = 2y^3 - 1$$

Evidentemente $2y^3 - 1$ es su propio resto al ser dividido entre $\{g_1, g_2, g_3\}$ luego añadimos $g_4 = 2y^3 - 1$ y repetimos el proceso:

$$S(g_1, g_2) = x = g_3 \equiv 0$$
$$S(g_2, g_3) = g_4 \equiv 0$$
$$S(g_1, g_3) = 2xy^2 = 2y^2g_3 \equiv 0$$
$$S(g_1, g_4) = x^2 + 4xy^5 = xg_3 + 4y^4g_2 \equiv 0$$
$$S(g_2, g_4) = x + 4y^5 - 2y^2 = g_3 + y^2g_4 \equiv 0$$
$$S(g_3, g_4) = x = g_3 \equiv 0$$

Luego el algoritmo termina y hemos encontrado la base de Gröbner

$$\{x^2 + 2xy^2, xy + 2y^3 - 1, x, 2y^3 - 1\}$$

Evidentemente está base de Gröbner no es reducida, todos los polinomios son monicos, pero $g_2 = yg_3 + g_4$ y $g_1 = (x + 2y)g_3$. Se puede comprobar que $\{x, 2y^3 - 1\}$ sí es la base de Gröbner reducida de I.

El Teorema de Eliminación

El teorema de eliminación nos da herramientas para resolver sistemas de ecuaciones polinómicas en varias variables.
Supongamos que $S = \{f_1, .., f_m\}$ es una colección de polinomios en $k[x_1, \ldots, x_n]$ y estamos intentando hallar valores de $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ para los cuales $f_1(a) = 0, f_2(a) = 0, \ldots, f_m(a) = 0$ es decir, esto es lo mismo que calcular $V = \mathcal{Z}(S)$. Como vimos que $\mathcal{Z}(S) = \mathcal{Z}(I)$ siendo $I = (S)$ el ideal generado por los elementos de S, es decir, los polinomios de I tienen las mismas raíces comunes que los polinomios de S.

En el caso de que $S = \{f_1, \ldots, f_m\}$ consista en polinomios lineales, podemos hallar $\mathcal{Z}(S)$ usando el método de eliminación gaussiana. El teorema de eliminación nos dice que calcular bases de Göbner es un método de llegar a resolver ecuaciones polinómicas más generales pues consigue lo mismo que la eliminación gaussiana para polinomios de grado más general.

Definición. Si I es un ideal en $k[x_1, ...x_n]$, entonces $I_i = I \cap k[x_1, \ldots, x_i]$ recibe el nombre de **i-ésimo ideal de eliminación de I**.

Teorema 12. *(Teorema de Eliminación)* Supongamos que $G = \{g_1, g_2, \ldots, g_m\}$ es una base de Gröbner para el ideal no nulo $I \subseteq k[x_1, x_2, \ldots, x_n]$ con respecto al orden monomial lexicográfico $x_1 > x_2 > \cdots > x_n$.
Entonces $G \cap k[x_{i+1}, \ldots, x_n]$ es una base de Gröbner del i-esimo ideal de eliminacion de I, $I_i = I \cap k[x_{i+1}, x_{i+2}, \ldots, x_n]$. En particular, $G \cap k[x_{i+1}, x_{i+2}, \ldots, x_n] = \emptyset$ si y solo si $I_i = 0$.

Supongamos ahora como al principio que tenemos $S = \{f_1, \ldots, f_m\}$, conjunto de polinomios de $k[x_1, \ldots, x_n]$ para los que queremos calcular $\mathcal{Z}(S)$. Usaremos el orden monomial lexicográfico $x_1 > x_2 > \cdots > x_n$

1. Pasamos a trabajar con $I = (S)$ porque el resultado no cambia.
2. Calculamos una base de Gröbner $\{g_1, g_2, \ldots, g_k\}$ de I (Usando el algoritmo de Buchberger).
3. Cogemos $G_{n-1} = G \cap k[x_n]$. Por el teorema de eliminación G_{n-1} genera $I_{n-1} = I \cap k[x_n]$. Si $G_{n-1} = \emptyset$ intentar usar G_{n-2} o otro anterior.
4. Resolvemos el sistema que nos haya salido, debería tendrá menos variables que el original. Idealmente querremos una sola variable.
5. Sustituimos lo que hayamos despejado en el paso anterior para poder resolver en casos anteriores. Así sucesivamente hasta resolver para todas las variables.

Ejemplo:

Vamos a buscar la solución al sistema de ecuaciones polinomicas en $\mathbb{R}[x, y]$:

$$\begin{cases} x^2 + xy - y^2 - 1 = 0 \\ x^2 + 4y^2 - 4 = 0 \end{cases}$$

Esto es equivalente a encontrar el conjunto algebraico afín de $I = (x^2 + xy - y^2 - 1, x^2 + 4y^2 - 4)$. Fijamos el orden monomial lexicografico $x > y$ obtenemos la base de Gröbner reducida de I:

$$\{g_1 = x - \frac{13}{3}y^3 + \frac{13}{3}y,\ g_2 = y^4 - \frac{22}{13}y^2 + \frac{9}{13}\}$$

Las soluciones del sistema tendrán que satisfacer que $g_1 = g_2 = 0$. Vemos que g_2 depende solo de una variable y, podemos encontrar sus raíces que nos darán los posibles valores de y para la solución. Dichas raíces son:

$$1,\ -1,\ \frac{3}{\sqrt{13}},\ -\frac{3}{\sqrt{13}}$$

Sustituyendo por esos valores en g_1 y despejando x acabamos de resolver el sistema. La solución son los puntos:

$$\begin{array}{cc} (0,1) & (0,-1) \\ (-\frac{4}{\sqrt{13}}, \frac{3}{\sqrt{13}}) & (\frac{4}{\sqrt{13}}, -\frac{3}{\sqrt{13}}) \end{array}$$

Cálculo de k-álgebras

Ahora vamos a dar una forma explícita de calcular el núcleo y la imagen de un homomorfismo de k-álgebras:

$$\phi\colon k[y_1,\dots,y_m]/J \to k[x_1,\dots,x_n]/I$$

siendo I, J ideales. Un caso concreto importante será $I=\mathcal{I}(V)$, $J=\mathcal{I}(W)$ con V, W conjuntos algebraicos afines en $\mathbb{A}^n$, $\mathbb{A}^m$ respectivamente.

Vamos a introducir algo de notación. Para $1\leq i\leq m$, sea $\varphi_i\in k[x_1,\dots,x_n]$ cualquier polinomio que represente a la clase de equivalencia de $\phi(\overline{y}_i)$. Observemos que dado $f(y_1,\dots,y_m)+J$ su imagen por ϕ es $f(\varphi_1,\dots,\varphi_m)+I$. Esto ocurre porque los $\overline{y}_1,\dots,\overline{y}_m$ generan $k[y_1,\dots,y_m]/J$ como k-álgebra y ϕ es un homomorfismo de k-álgebras.

Proposición 13. Con la notación anterior. Sea $R=k[y_1,\dots,y_m,x_1,\dots,x_n]$ y sea $\mathcal{A}$ el ideal generado por $y_1-\varphi_1,\dots,y_m-\varphi_m$ junto a un conjunto generador de I. Sea G la base reducida de Gröbner de $\mathcal{A}$ respecto al orden monomial lexicográfico $x_1>\cdots>x_n>y_1>\cdots>y_n$.

1. El núcleo de ϕ es $\mathcal{A}\cap k[y_1,\dots,y_m]$ modulo J. Los elementos de G en $k[y_1,\dots,y_m]$ (también modulo J) generan $ker(\phi)$.
2. Si $f\in k[x_1,\dots,x_n]$, entonces $\overline{f}$ está en la imagen de ϕ si y solo el resto tras aplicar el algoritmo general de la división de f entre los elementos de G es un elemento $h\in k[y_1,\dots,y_m]$, en cuyo caso $\phi(\overline{h})=f$

Demostración:

1. *Si probamos que $\ker\phi=\mathcal{A}\cap k[y_1,\dots,y_m]$ la segunda parte saldrá inmediatamente del teorema de eliminación.*

Sean $f\in\mathcal{A}\cap k[y_1,\dots,y_m]$ y sean $f_1,\dots,f_s$ generadores de I en $k[x_1,\dots,x_n]$. Entonces como $f\in\mathcal{A}$ y usando los generadores de $\mathcal{A}$:

$$f(y_1,\dots,y_m)=\sum a_i(y_i-\varphi_i)+\sum b_if_i\quad a_i,b_i\in R$$

Sustituyendo y_i por φ_i

$$f(\varphi_1,\dots,\varphi_m)=\sum a_i(\varphi_i-\varphi_i)+\sum b_if_i=\sum b_if_i\in I$$

Como $\phi(\overline{f})=f(\varphi_1,\dots,\varphi_m)\ mod\, I$ tenemos que $\phi(\overline{f})=0\ mod\, I$ luego $\overline{f}\in\ker\phi$, f representa una clase de equivalencia en $\ker\phi$.

Veamos que $\ker\phi\subseteq\mathcal{A}\cap k[y_1,\dots,y_m]$. Supongamos que $f\in k[y_1,\dots,y_m]$ representa a un elemento de $ker\,(\phi)$. Entonces $f(\varphi_1,\dots,\varphi_m)\in I$ (en $k[x_1,\dots,x_n]$) luego también $f(\varphi_1,\dots,\varphi_m)\in\mathcal{A}$. Como $y_i-\varphi_i=a_i\in\mathcal{A}$ entonces $f(y_1,\dots,y_m)=\sum k_jy_1^{p_{j,1}}\dots y_m^{p_{j,m}}=\sum k_j(\varphi_1+a_1)^{p_{j,1}}\dots(\varphi_m+a_m)^{p_{j,m}}$. Operando esta expresión y sabiendo que como $\mathcal{A}$ es un ideal cualquier término a_i absorberá dentro de $\mathcal{A}$ cualquier producto en el que aparezca:

$$\sum k_j\varphi_1^{p_{j,1}}\dots\varphi_m^{p_{j,m}}+\mathcal{A}=f(\varphi_1,\dots,\varphi_m)+\mathcal{A}$$

Luego:

$$f(y_1,\dots,y_m)\equiv f(\varphi_1,\dots,\varphi_m)\equiv 0\ mod\,\mathcal{A}$$

Es decir, $f \in \mathcal{A} \cap k[y_1, \ldots, y_m]$ acabando de probar (1).

2. *Supongamos que $f \in k[x_1, \ldots, x_n]$ tal que $\overline{f} \in Im\,\phi$ y existe $h \in k[y_1, \ldots, y_m]$ $\phi(\overline{h}) = \overline{f}$. Entonces:*

$$f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in I$$

como polinomios de $k[x_1, \ldots, x_n]$. Por tanto $f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in \mathcal{A}$ como polinomios de R. Como antes tenemos que:

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) \in \mathcal{A}$$

Entonces f y h dejan el mismo resto al aplicarles el algoritmo general de la división por G. Como tenemos el orden monomial dado por $x_1 > \cdots > x_n > y_1 > \cdots > y_m$ el resto de $h(y_1, \ldots, y_m)$ tiene que ser un polinomio h_0 que solo dependa de las variables $y_1, \ldots, y_m$. También es importante que $h - h_0 \in \mathcal{A} \cap k[y_1, \ldots, y_m] = ker\,\phi$ luego $\phi(\overline{h_0}) = \phi(\overline{h}) = \overline{f}$.

Al revés, si f deja resto h después del algoritmo general de la división por G entonces $f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) \in \mathcal{A}$.

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = \sum a_i(y_i - \varphi_i) + \sum b_i f_i)$$

como polinomios de R. Sustituyendo y_i por φ_i:

$$f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in I \quad \textit{como polinomios de } k[x_1, \ldots, x_n]$$

Luego $\overline{f} = \phi(\overline{h})$. ∎

Corolario 14. La aplicación ϕ es suprayectiva si y solo si para cada i, $1 \leq i \leq n$, la base de Gröbner reducida contiene un polinomio $x_i - h_i$ con $h_i \in k[y_1, \ldots, y_m]$.

Ejemplo:

Definimos $\widetilde{\varphi}\colon \mathbb{Q}[u, v, w] \to \mathbb{Q}[x, y]$ el homomorfismo de anillos inducido por el morfismo $\varphi\colon \mathbb{Q}^2 \to \mathbb{Q}^3$, $\varphi(x, y) = (x^2 + y, x + y^2, x - y)$. Notemos que $\mathcal{I}(\mathbb{Q}^2) = (0) \in \mathbb{Q}[x, y]$ luego $\mathbb{Q}[x, y] = \mathbb{Q}[x, y]/\mathcal{I}(\mathbb{Q}^2)$. Podemos hacer lo mismo para $\mathbb{Q}[u, v, w]$.

Calculemos el núcleo de $\widetilde{\varphi}$. Para ello definimos el ideal $\mathcal{A} = (u - x^2 - y, v - x - y^2, w - x + y, 0) \in \mathbb{Q}[u, v, w, x, y]$ y fijamos el orden monomial lexicografico $x > y > u > v > w$. Calculamos G la base de Gröbner reducida de $\mathcal{A}$ respecto a ese orden monomial:

$$\begin{aligned}
&x - y - w \\
&y^2 + y - v + w \\
&yu - yv - \frac{1}{2}uw + \frac{3}{2}u - \frac{3}{2}vw - \frac{3}{2}v + \frac{1}{2}w^3 + \frac{3}{2}w \\
&yw - \frac{1}{2}u + \frac{1}{2}v + \frac{1}{2}w^2 - \frac{1}{2}w \\
&u^2 + 2uv - 2uw^2 - 4vw + w^4 + 3w^2
\end{aligned}$$

Vemos que $G \cap \mathbb{Q}[u, v, w] = \{u^2 + 2uv - 2uw^2 - 4vw + w^4 + 3w^2\}$ luego por la Proposición 13 tenemos que $ker\,\varphi = (u^2 + 2uv - 2uw^2 - 4vw + w^4 + 3w^2)$.

Ahora vamos a ver si $f = 2x^3 - 4xy - 2y^3 - 4y$ está en la imagen de φ. Para ello aplicamos el algoritmo general de la división para f entre G que da resto $h = 3uw - 5u + 3vw + v - w^3 + 2w^2 - w \in \mathbb{Q}[u, v, w]$. Por la Proposición 13 tendremos que $\varphi(h) = f$.

2 Radicales y variedades afines

En general en un anillo de polinomios $k[x_1, x_2, \ldots, x_n]$ un conjunto algebraico afín puede ser generado por muchos ideales distintos. En concreto los ceros de un polinomio f son exactamente los mismos que los de sus potencias $f^2, f^3, \ldots$

Definición. Sea I un ideal en un anillo conmutativo R.

- El **radical** de I, denotado $rad\, I$, es el conjunto de elementos de R para los cuales alguna de sus potencias estará en I.

$$rad\, I = \{a \in R \mid a^k \in I \text{ para algún } k \geq 1\}$$

- Un ideal que coincide con su radical se denomina **ideal radical**.
- El radical del ideal nulo $rad(0)$ se denomina **nilradical** y está formado por aquellos elementos a para los cuales algunas de sus potencias se anula $a^k = 0$. Dichos elementos se llaman elementos **nilpontentes**.

Proposición 15. Sea I un ideal en un anillo conmutativo R.

1. $rad\, I$ es un ideal que contiene a I.
2. $rad\, I/I$ es el nilradical de R/I.
3. El radical de la intersección finita de ideales es la intersección finita de los radicales correspondientes.

Demostración:

2. *Que $I \subseteq rad\, I$ es evidente. Por definición de nilradical, los elementos en el nilradical de R/I son elementos $a + I$ tales que $(a + I)^n = a^n + I = 0$ para algún entero positivo n, es decir $a^n \in I$. Esto es lo mismo que decir que $a \in rad\, I$ o (pasando al anillo cociente) que $a \in rad\, I/R$. Luego $rad\, I/I$ es el nilradical de R/I.*

1. *Ahora si demostramos que N el nilradical de un anillo conmutativo R, es un ideal (y por tanto, que $rad(I)/I$ es un ideal de R/I), aplicando el cuarto teorema de isomorfía tendremos* 1.

Empezamos viendo que $N \neq \emptyset$ ya que $0 \in N$. Ahora con $a \in N$ y $r \in R$, vemos que $ar \in N$ ya que por definición de N existe $k \geq 1$ tal que $a^k = 0$ y por tanto $(ar)^k = a^k r^k = 0r^k = 0$. Por último, siendo $a, b \in N$ veamos que $a + b \in N$. Por definición de N existen n, m tal que $a^n = b^m = 0$. Como la fórmula del binomio de Newton funciona en R:

$$(a + b)^{n+m} = \sum_{i=0}^{n+m} r_i a^i b^{n+m-i}$$

Es sencillo ver que para cualquier valor de i, $0 \leq i \leq n + m$ o bien $i \geq n$ o $n + m - i \geq m$, por tanto en todos los sumandos $a^i = 0$ o $b^{n+m-i} = 0$ luego todos los sumandos son cero, el sumatorio es cero y $a + b \in N$.

3. *Sean Q, J ideales de R. Que $rad\,(Q \cap J) \subseteq rad\, Q \cap rad\, J$ es trivial. Al revés, sea $a \in rad\, Q \cap rad\, J$, eso quiere decir que para dos enteros positivos q, j, $a^q \in Q$ y $a^j \in J$. Pero eso implica que $a^{qj} \in Q \cap J$ luego $a \in rad\,(Q \cap J)$. Generalizar a la intersección finita es sencillo porque la intersección es asociativa.* ∎

Alguna observación sobre el resultado anterior:

- Es inmediato de (2) que un ideal I es radical si y solo si R/I no tiene elementos nilpotentes.
- Ya en la demostración del resultado vemos cuál va ser nuestro principal uso para la afirmación (2). Nos permite probar resultados generales para radicales estudiando el caso concreto del nilradical.

El siguiente resultado va a ser uno de los más utilizados cuando trabajemos con radicales de aquí en adelante.

Proposición 16. El radical de un ideal propio I es la intersección de todos los ideales primos que contienen a I. En particular, el nilradical es la intersección de todos los ideales primos.

Demostración:

Primero pasamos a estudiar R/I. Por la Proposición 15.(2) *y el cuarto teorema de isomorfía vemos que $rad\,(I)$ será la intersección de todos los ideales primos de R que contienen a I si y solo si el nilradical de R/I es la intersección de todos los ideales primos de R/I.*

Sea N el nilradical de un anillo conmutativo R. Sea N' la intersección de todos los ideales primos de R.

$\underline{N \subseteq N'}$ Sea $a \in N$, sea P un ideal primo cualquiera, veamos que $a \in P$. Como $a \in N$ existe k un entero mayor que cero tal que $a^k \in P$ porque para algún k $a^k = 0$ que siempre está en P, escojamos n el menor entero para el que $a^n \in P$. $a^n = a^{n-1}a \in P$ y como P es un ideal primo o bien $a \in P$ o $a^{n-1} \in P$ en este segundo caso violaríamos la minimalidad de n luego necesariamente $a \in P$ y $n = 1$. Por tanto $N \subseteq N'$.

$\underline{N' \subseteq N}$ Probaremos que si $a \notin N$ entonces $a \notin N'$. Sea $a \notin N$ y sea S la familia de todos los ideales propios de R que no contienen a ninguna potencia de a. S no es vacío porque $(0) \in S$. Además si $I_1 \subseteq I_2 \subseteq \cdots$ es una cadena ascendente de ideales de S entonces $\cup I_i$ también estará en S, por tanto S tiene cotas superiores para sus cadenas y por el lema de Zornn, algún elemento maximal que denotaremos P. Veamos que P es primo, supongamos que $x, y \notin P$ pero $xy \in P$, entonces por la maximalidad de P en S, $a^n \in (x) + P \notin S$ y $a^m \in (y) + P \notin S$ para ciertos enteros n, m. $a^{nm} \in (xy) + P = P$ lo cual es contradictorio con que $P \in S$. Como P es un primo en S $a \notin N'$. ■

Corolario 17. Los ideales primos (y por tanto también los maximales) son radicales.

Proposición 18. Si R es un anillo noetheriano entonces para cualquier ideal I alguna potencia positiva de $rad\,I$ esta contenida en I.

2.1 La Topología de Zariski

Observamos en la sección 1 que los conjuntos algebraicos afines cumplían las condiciones necesarias para definir los cerrados de una topología en $\mathbb{A}^n$. Recordemos:

1. La intersección arbitraria de conjuntos algebraicos afines es un conjunto algebraico afín.

2. Las uniones finitas de conjuntos algebraicos afines es un conjunto algebraico afín

3. $\mathbb{A}^n$ y $\emptyset$ son conjuntos algebraicos afines.

Definición. La topología en el conjunto $\mathbb{A}^n$ sobre un cuerpo k cuyos conjuntos cerrados son los conjuntos algebraicos afines recibe el nombre de **topología de Zariski**.

Recordemos que como los conjuntos algebraicos afines son los cerrados de la topología de Zariski entonces sus complementarios conformarán los conjuntos abiertos.

En este trabajo no estudiaremos la topología de Zariski en gran profundidad. Dos propiedades importantes son: cada punto es un conjunto cerrado (ya vimos que todo punto era conjunto algebraico afín) y cuando $\mathbb{A}^1 = k$ con k un cuerpo infinito la intersección de dos abiertos no vacios nunca es vacía. Consecuencias inmediatas de dichas propiedades es que la topología de Zariski siempre es T_1 y si k es infinito la topología de Zariski de $\mathbb{A}^1$ nunca es T_2.

Sea $\mathbb{A}^1 = k$ con k un cuerpo infinito, supongamos que $A_1 = \mathcal{Z}(I_1)^c$, $A_2 = \mathcal{Z}(I_2)^c$(I_1, I_2 ideales de $k[\mathbb{A}^1]$) son abiertos en la topología de Zariski de $\mathbb{A}^1$ tales que $A_1, A_2 \neq \emptyset$ y $A_1 \cap A_2 = \emptyset$. En ese caso por las leyes de Morgan y las propiedades de $\mathcal{Z}$, $A_1 \cap A_2 = (\mathcal{Z}(I_1) \cup \mathcal{Z}(I_2))^c = \mathcal{Z}(I_1 I_2)^c$ luego $\mathcal{Z}(I_1 I_2) = \mathbb{A}^1$ y al ser k infinito $I_1 I_2 \subseteq \mathcal{I}(\mathbb{A}^1) = (0)$ luego $I_1 I_2 = (0)$ y como $k[\mathbb{A}^1]$ es un dominio de integridad tenemos que I_1 o I_2 es igual a (0), sin perdida de generalidad elegimos $I_1 = (0)$ en cuyo caso $A_1 = \mathcal{Z}(I_1)^c = \mathcal{Z}(0)^c = (\mathbb{A}^1)^c = \emptyset$ llegando a una contradicción.

Además nos interesa definir la topología de Zariski relativa a los conjuntos algebraicos $V \subseteq \mathbb{A}^n$. Para esto necesitamos extender la definición de $\mathcal{Z}$ e $\mathcal{I}$ al anillo de coordenadas $k[V]$.

Nota:*(Extensión de las definiciones de $\mathcal{Z}$ e $\mathcal{I}$)*

Primero consideremos $k[V]$ como el conjunto de funciones distintas que surgen de restringir funciones de $k[\mathbb{A}^n]$ a ser evaluadas solo en V tal y como vimos en la sección 1. Visto de esta forma hay una manera natural de extender las definiciones de $\mathcal{Z}$ e $\mathcal{I}$:

$$\mathcal{Z}\colon \{\text{ideales en } k[V]\} \longrightarrow \{\text{conjuntos algebraicos de } V\}$$
$$\mathcal{I}\colon \{\text{subconjuntos de } V\} \longrightarrow \{\text{ideales de } k[V]\}$$

Si $\overline{J}$ es un ideal en $k[V]$ entonces $\mathcal{Z}(\overline{J})$ son los puntos de V en los que se anulan todos los elementos de $\overline{J}$. Por otro lado si $B \subseteq V$, $\mathcal{I}(B)$ será todos los elementos de $k[V]$ que se anulan en todos los puntos de B.

Es fácil comprobar que esta nueva definición de $\mathcal{Z}$ sigue verificando las propiedades para poder definir los cerrados de una topología en V. Definimos pues la topología de Zariski en V como la topología que tiene como cerrados a los conjuntos de la forma $\mathcal{Z}(\overline{J})$ con $\overline{J}$ ideal en $k[V]$.

Si J es la preimagen de $\overline{J}$ en $k[\mathbb{A}^n]$ tenemos que $\mathcal{Z}(J) \cap V = \mathcal{Z}(\overline{J})$ (los elementos de $\overline{J}$ surgen de restringir los elementos de J a ser evaluados en V). Por tanto vemos que la topología que hemos definido para V coincide con su topología de subconjunto dentro

de la topología de Zariski de $\mathbb{A}^n$. Notemos que nuestra definición no requiere conocer que conjunto contiene a V lo que suele ser más conveniente.

Si V y W son dos conjuntos algebraicos afines y $\varphi\colon V \to W$ un morfismo entre ellos, es fácil ver que φ es una función continua respecto a sus topologías de Zariski (si $\widetilde{\varphi}$ es el homomorfismo asociado a φ se puede comprobar que si W' es un subconjunto algebraico de W, con $\mathcal{Z}(I) = W'$, entonces $V' = \mathcal{Z}(\widetilde{\varphi}(I))$ verifica que $\varphi^{-1}(W') = V'$). Esto no quiere decir que todas la aplicaciones continuas entre V y W sean morfismos.

Estudiemos ahora un par de conceptos asociados a topologías en relación a la topología de Zariski.

Definición. Para cualquier subconjunto A de $\mathbb{A}^n$, la **clausura de Zariski** de A, $Cl(A)$, es el menor conjunto algebraico que contiene a A. Si $A \subseteq V$ para V un conjunto algebraico, A es **denso** en V si la clausura de A es V.

Proposición 19. La clausura de Zariski de un subconjunto A en $\mathbb{A}^n$ es $\mathcal{Z}(\mathcal{I}(A))$.

Demostración:

Ya sabemos que $A \subseteq \mathcal{Z}(\mathcal{I}(A))$. Si V es un conjunto algebraico que contiene a A entonces $\mathcal{I}(V) \subseteq \mathcal{I}(A)$ luego $\mathcal{Z}(\mathcal{I}(A)) \subseteq \mathcal{Z}(\mathcal{I}(V))$. ∎

Proposición 20. Supongamos que $\varphi\colon V \to W$ es un morfismo de conjuntos algebraicos y que $\widetilde{\varphi}\colon k[W] \to k[V]$ es el homomorfismo de k-álgebras asociado a φ. Entonces:

1. El núcleo de $\widetilde{\varphi}$ es $\mathcal{I}(\varphi(V))$.
2. La clausura de Zariski de $\varphi(V)$ es $\mathcal{Z}(ker\,\widetilde{\varphi})$ en W. En particular, $\widetilde{\varphi}$ es inyectiva si y solo si $\varphi(V)$ es denso en W.

Demostración:

1. $\widetilde{\varphi}(f) = f \circ \varphi$ luego $\widetilde{\varphi}(f) = 0$ equivale a que $(f \circ \varphi)(p) = 0$ para todo punto p de V o lo que es lo mismo, $f(q) = 0$ para todo punto $q = \varphi(p) \in \varphi(V)$, $f \in \mathcal{I}(\varphi(V))$.

2. Por la Proposición 19 la clausura de $\varphi(V)$ es $\mathcal{Z}(\mathcal{I}(\varphi(V)))$ pero por (1) tenemos que $\mathcal{I}(\varphi(V)) = ker\,\widetilde{\varphi}$ luego $Cl(\varphi(V)) = \mathcal{Z}(ker\,\widetilde{\varphi})$. Para la segunda afirmación $ker\,\widetilde{\varphi} = 0$ implicaría que $\mathcal{Z}(ker\,\widetilde{\varphi}) = \mathcal{Z}(0) = W = Cl(\varphi(V))$. ∎

2.2 Variedades afines

En esta subsección estudiaremos si los conjuntos algebraicos afines pueden ser descompuestos como uniones de otros subconjuntos algebraicos más pequeños. Esto sería encontrar una base para los cerrados de la topología de Zariski.

Definición. Un conjunto algebraico afín no vacío V es **irreducible** si no puede ser expresado como unión $V = V_1 \cup V_2$ de dos conjuntos algebraicos afines V_1, V_2 distintos de V. Los conjuntos algebraicos afines irreducibles reciben el nombre de **variedades** o variedades afines.

Proposición 21. Sea V un conjunto algebraico afín de $\mathbb{A}^n$ sobre un cuerpo k.

1. V es irreducible si y solo si $\mathcal{I}(V)$ es un ideal primo

2. Si V no es vacío entonces puede ser expresado de manera única de la forma:

$$V = V_1 \cup V_2 \cup \cdots \cup V_q$$

siendo $V_1, V_2, \ldots, V_q$ variedades afines entre las cuales se cumple $V_i \nsubseteq V_j$ si $i \neq j$ (No hay elementos superfluos).

Demostración:

1. Supongamos que V no es irreducible, $V = V_1 \cup V_2$, además definimos $I = \mathcal{I}(V)$.En ese caso como $V_1 \neq V$, existe f_1 que se anula en todo V_1 pero no en todo V es decir $f_1 \in \mathcal{I}(V_1) - I$, igualmente existe $f_2 \in \mathcal{I}(V_2) - I$. Como $V = V_1 \cup V_2$, $f_1 f_2$ se anula en todo V luego $f_1 f_2 \in I$, por tanto I no es primo si V no es irreducible.

Al revés, si I no es primo existen $f_1, f_2 \in k[\mathbb{A}^n]$ tal que $f_1 f_2 \in I$, $f_1, f_2 \notin I$. Sea $V_1 = \mathcal{Z}(f_1) \cap V$ y $V_2 = \mathcal{Z}(f_2) \cap V$ que son conjuntos algebraicos. Como ni f_1 ni f_2 se anulan en V tenemos que V_1, V_2 son distintos de V pero como $f_1 f_2 \in I$ tenemos que $V \subseteq \mathcal{Z}(f_1 f_2) = \mathcal{Z}(f_1) \cup \mathcal{Z}(f_2)$ y por tanto $V = (\mathcal{Z}(f_1) \cup \mathcal{Z}(f_2)) \cap V = (\mathcal{Z}(f_1) \cap V) \cup (\mathcal{Z}(f_2) \cap V) = V_1 \cup V_2$. Luego V no es irreducible.

Que V no sea irreducible si y solo si $\mathcal{I}(V)$ no es primo es equivalente a que V sea irreducible si y solo si $\mathcal{I}(V)$ es primo.

2. Sea S la colección de conjuntos algebraicos de $\mathbb{A}^n$ que no pueden ser expresados como unión finita de conjuntos algebraicos irreducibles. Supongamos que $S \neq \emptyset$. S induce una familia de ideales en $k[\mathbb{A}^n]$, $S' := \{\mathcal{I}(V) \mid V \in S\}$ que al ser $k[\mathbb{A}^n]$ noetheriano tendrá un elemento maximal I_0 por el Teorema 2. Entonces $V_0 = \mathcal{Z}(I_0)$ es un elementos minimal de S. Si V_0 fuese irreducible no estaría en S porque sería su propia descomposición. Por otro lado si $V_0 = V_1 \cup V_2$, con V_1 o V_2 en S sería una contradicción con el hecho de que V_0 es minimal en S, pero si $V_1, V_2 \notin S$, V_1, V_2 tendrían sus propias descomposiciones que al juntarlas darían la de V_0. En cualquier caso llegaríamos a una contradicción, por tanto $S = \emptyset$. Todo conjunto algebraico puede ser expresado como unión de variedades afines. $V_i \nsubseteq V_j$ es inmediato porque en caso contrario podríamos eliminar V_i de la unión sin alterar el resultado.

Supongamos ahora que V tiene dos descomposiciones en variedades afines:

$$V = V_1 \cup V_2 \cup \cdots \cup V_r = U_1 \cup U_2 \cup \cdots \cup U_t$$

Entonces:

$$V_1 \subseteq U_1 \cup U_2 \cup \cdots \cup U_t$$

y cada $V_1 \cap U_i$, $i = 1, \ldots, t$ es algebraico luego:

$$V_1 = (V_1 \cap U_1) \cup (V_1 \cap U_2) \cup \cdots \cup (V_1 \cap U_t)$$

contradice que V_1 sea irreducible a no ser que $V_1 = U_i$ para algún $i \in \{1, \ldots, t\}$. Se puede aplicar el mismo argumento a todos los demás V_j y a todos los U_i para ver que efectivamente las dos descomposiciones son iguales. ■

Corolario 22. Un conjunto algebraico afín V es una variedad si y solo si su anillo de coordenadas $k[V]$ es un dominio de integridad. Esto equivale a decir que V es una variedad si y solo si $\mathcal{I}(V)$ es un ideal primo.

Ejemplo:

Sea $\mathbb{R}^2$. $\mathcal{Z}(xy)$ no es una variedad afín, basta ver que en $\mathbb{R}^2/(xy)$ tenemos que $\overline{x} * \overline{y} = \overline{0}$ luego existen divisores de cero. Tenemos que $\mathcal{Z}(xy) = \mathcal{Z}(x) \cup \mathcal{Z}(y)$.

2.3 Descomposición primaria de ideales en anillos noetherianos

Como vimos en la sección 1, los ideales de un anillo de polinomios $k[x_1, \ldots, x_n]$ sobre un cuerpo k están relacionados con los conjuntos algebraicos afines de $\mathbb{A}^n$ sobre k. Hemos visto que los conjuntos algebraicos afines se podían descomponer de manera única en variedades algebraicas. Nos preguntamos ahora si se podría hacer algo equivalente para los ideales de $k[x_1, \ldots, x_n]$.

Definición. Un ideal propio Q en un anillo conmutativo R es **primario** si para cada $ab \in Q$, si $a \notin Q$ entonces $b \in rad\, Q$.

Esta definición se parece mucho a la de los ideales primos, de hecho todos los ideales primos son primarios (porque son radicales). Veamos algunas propiedades esenciales de los ideales primarios.

Proposición 23. Sea R un anillo conmutativo y unitario

1. Un ideal Q es primario si y solo si todos los divisores de cero en R/Q son nilpotentes.
2. Si Q es un ideal primario entonces $rad\, Q$ es un ideal primo.
3. Si Q es un ideal con $rad\, Q$ un ideal maximal, entonces Q es un ideal primario.
4. Supongamos que M es un ideal maximal y que Q es un ideal tal que $M^n \subseteq Q \subseteq M$ para n algún entero positivo. Entonces Q es un ideal primario con $rad\, Q = M$.

Demostración:

1. *Sale directamente de la definición de primario y de la Proposición* 15.(2).

2. *Supongamos que* $ab \in rad\, Q$. *Entonces* $a^m b^m = (ab)^m$ *y como* Q *es primario tendremos que* $a^m \in Q \subseteq rad\, Q$ *o* $b^m \in rad\, Q$.

3. *Pasando a* R/Q *y con el apartado* (1) *solo necesitamos probar que si el nilradical de un anillo conmutativo es maximal todo divisor de cero es nilpotente. Vimos en la Proposición* 16 *que el nilradical está contenido en todos los ideales primos de dicho anillo, por tanto si el nilradical es maximal será el único ideal maximal del anillo. Si* d *es un divisor de cero entonces* (d) *es un ideal propio que tiene que estar contenido en un ideal maximal. El único ideal maximal en este caso el nilradical luego* d *será nilpotente.*

4. *Como* $Q \subseteq M$ *tenemos que* $rad\, Q \subseteq rad\, M = M$. *Como* $M^n \subseteq Q$ *tenemos que* $rad\, M \subseteq rad\, Q$. *Por tanto,* $rad\, Q = M$ *que es un ideal maximal, aplicando el apartado* (3) Q *será un ideal primario.* ∎

Notemos que si Q es primario entonces $rad\, Q$ es el menor ideal primo que contiene a Q porque es la intersección de todos los ideales primos que contienen a Q.

Definición. Si Q es un ideal primario, entonces el ideal primo $P := rad\, Q$ recibe el nombre de **primo asociado** a Q. A su vez se dice que Q es P-primario.

Corolario 24. La intersección finita de ideales P-primarios es P-primaria.

Demostración:

Es inmediata a partir de la Proposición 15.(3). ∎

Ejemplo:

Para cualquier cuerpo k, el ideal (x) en $k[x, y]$ es primario ya que es primo. A su vez el ideal $(x, y)^n$ es primario ya que es potencia del ideal maximal (x, y).

Definición. Un ideal, I, en un anillo conmutativo R tiene una **descomposición primaria** si puede expresarse como intersección finita de ideales primarios.

$$I = \bigcap_{i=1}^{m} Q_i \qquad Q_i \text{ ideal primario}$$

Además dicha descomposición se dice **mínima** y los Q_i son **componentes primarias** de I si:

1. Ningún ideal primario contiene a la intersección de todos los demás (no hay ningún elemento superfluo para la intersección).
2. Los primos asociados son distintos para cada Q_i, $rad\, Q_i \neq rad\, Q_j$ si $i \neq j$. (por el Corolario 24 varias componentes con el mismo primo asociado pueden sustituirse por su intersección para obtener una descomposición primaria con menos elementos).

Veamos que en anillos noetherianos siempre existe una descomposición primaria mínima para todos los ideales. Es fácil comprobar que a partir de una descomposición primaria cualquiera se puede obtener una descomposición primaria mínima.

Definición. Un ideal propio, I, de un anillo conmutativo R se dice **irreducible** si no puede se expresado como la intersección no trivial de dos ideales, es decir, si $I = J \cap K$ entonces $I = J$ o $I = K$.

Todo ideal primo es irreducible. Veámoslo por reducción al absurdo: supongamos que P es un ideal primo reducible $P = J \cap K$ y $P \neq J$, $P \neq K$. Luego existen $a \in J - P$ y $b \in K - P$ para los cuales $ab \in J \cap K = P$ y al ser P primo algún a o b deberá estar en P lo cual nos lleva a una contradicción.

Proposición 25. Sea R un anillo noetheriano.

1. Todo ideal irreducible es primario.
2. Todo ideal propio de R es intersección finita de ideales irreducibles.

Demostración:

1. *Sea Q un ideal irreducible y supongamos que $ab \in Q$ y $b \notin Q$. Es fácil ver que si fijamos un entero positivo n, el conjunto $\{x \in R \mid a^n x \in Q\}$ es un ideal que llamaremos A_n. Obviamente $A_1 \subseteq A_2 \subseteq \ldots$ y como R es noetheriano la cadena tiene que estabilizarse a partir de algún m.*

Consideremos $I = (a^m) + Q$ y $J = (b) + Q$ ideales en R, ambos conteniendo a Q. Si $y \in I \cap J$ entonces como y es elemento de I podemos expresar $y = a^m z + q$ para $z \in R$ y $q \in Q$. Hemos asumido que $ab \in Q$ luego $aJ \subseteq Q$, en particular $ay \in Q$. Podemos despejar $a^{m+1}z = ay - aq \in Q$ lo que nos lleva a que $z \in A_{m+1} = A_m$. Pero $z \in A_m$ quiere decir que $a^m z \in Q$, luego $y \in Q$. Tenemos entonces que $I \cap J = Q$. Como Q se supone irreducible esto solo será posible si $J = Q$ o $I = Q$. $b \notin Q$ luego $J \neq Q$ luego es necesario que $I = Q$, $I = (a^m) + Q = Q$ si y solo si $a^m \in Q$ o lo que es lo mismo, si $a \in \operatorname{rad} Q$.

2. *Está demostración es prácticamente idéntica a la de la Proposición 21.*

Definimos S como la familia de ideales propios de R que no se pueden expresar como intersección finita de ideales irreducibles. Suponemos que $S \neq \emptyset$ en cuyo caso, al ser R noetheriano, S tendrá un elemento maximal M. Al estar M en S no podrá ser él mismo irreducible, luego será intersección de dos ideales I, J que por la maximalidad de M no estarán en S. Como $I, J \notin S$ podrán ser expresados como intersecciones finitas de ideales irreducibles que al juntarse darán una expresión de M como intersección finita de ideales irreducibles, llegando a una contradicción. Por tanto tendremos que $S = \emptyset$, es decir todo ideal propio se puede expresar como intersección finita de ideales irreducibles. ∎

Este resultado nos asegura la existencia de la descomposición primaria pero no su unicidad. De hecho en general no existe descomposición primaria única. Sin embargo, sí podemos encontrar una propiedad que todas las descomposiciones primarias de un ideal deben compartir.

Teorema 26. (*de Descomposición Primaria*) Sea R un anillo noetheriano. Todo ideal I en R tiene al menos una descomposición primaria mínima. Sean dos descomposiciones primarias mínimas de I:

$$I = \bigcap_{i=1}^{m} Q_i = \bigcap_{i=i}^{n} Q'_i$$

Los conjuntos de primos asociados a las componentes de cada descomposición coinciden:

$$\{\operatorname{rad} Q_1, \operatorname{rad} Q_2, \ldots, \operatorname{rad} Q_m\} = \{\operatorname{rad} Q'_1, \operatorname{rad} Q'_2, \ldots, \operatorname{rad} Q'_n\}$$

Todavía más, los ideales primarios Q_i que pertenecen a los elementos mínimos de dicho conjunto están unívocamente determinados por I.

Demostración:

Demostraremos solo la primera afirmación.

Sea I un ideal en R y $a \in R$, definimos:

$$I_a := \{r \in R \mid ra \in I\}$$

y vemos algunas propiedades para este conjunto:

1. *I_a es un ideal: sea $r \in R$, $k \in I_a$, entonces como I es un ideal y $ka \in I$, $rka \in I$. Sean $k, r \in I_a$ entonces $ka \in I$ y $ra \in I$ luego $(k+r)a = ka + ra \in I$*
2. *$(I \cap J)_a = I_a \cap J_a$: Es sencillo por doble contenido.*
3. *Si I es un ideal P-primario y $a \notin I$, entonces I_a es P-primario. Si $a \notin P$, $I_a = I$:*
   - *Sea $b \in \operatorname{rad} I_a$ si y solo si $b^n \in I_a$ si y solo si $b^n a \in I$. Como I es P-primario y $a \notin I$ esto ocurre solo si $b^{nm} \in I$, o lo que es lo mismo, si $b \in P$. Por tanto $P = \operatorname{rad} I_a$. Supongamos que $cb \in I_a$ con $b \notin I_a$, entonces $cba \in I$ y al ser I primario y $ba \notin I$ tenemos que $c \in \operatorname{rad} I = P = \operatorname{rad} I_a$, luego I_a es P-primario.*
   - *Sea $a \notin P$ (y por tanto $a \notin I$) y $b \in I_a$. Como $ba \in I$ y I es primario, si $b \notin I$ tendríamos que $a \in \operatorname{rad} I = P$ lo cual no ocurre, por tanto $I_a \subseteq I$ y el contenido inverso es inmediato ya que I es un ideal.*

Ahora dada una descomposición primaria mínima cualquiera de I:

$$I = Q_q \cap Q_2 \cap \cdots \cap Q_m$$

Sea P_i el ideal primo asociado a Q_i.

Observemos que $I_a = (Q_1)_a \cap (Q_2)_a \cap \cdots \cap (Q_m)_a$ (por la propiedad 2). Como el radical de la intersección es igual a la intersección de los radicales (Proposición 15.3) $rad(I_a) = rad\,(Q_1)_a \cap \cdots \cap rad\,(Q_m)_a$.

Por la propiedad 3, $rad(Q_i)_a = rad(Q_i) = P_i$ si $a \notin Q_i$ y es evidente que si $a \in Q$, $Q_a = R$ luego $\operatorname{rad} Q_a = R$.

Sea Λ_a el conjuntos de índices de aquellos Q_i para los cuales $a \notin Q_i$. Es evidente que:

$$rad\, I_a = \bigcap_{i \in \Lambda_a} rad\,(Q_i)a = \bigcap_{i \in \Lambda_a} rad\, Q_i$$

Consideremos el conjunto:

$$J := \{rad\, I_a \mid a \in R\}$$

Veamos que existe $a_i \in R$ tal que $a_i \notin Q_i$ y $a \in \bigcap_{j \neq i} Q_j$. Por reducción al absurdo si no existiese a_i tendríamos que $\bigcap_{j \neq i} Q_j \subseteq Q_i$ en cuyo caso la descomposición no sería minimal lo cual es una contradicción. Observemos ahora que $\operatorname{rad} I_{a_i} = \operatorname{rad} Q_i = P_i$ lo que nos lleva a que $\{P_1, P_2, \ldots, P_m\} \subseteq J$.

Por otro lado, como cada I_a es un ideal primario (propiedad 3), $\operatorname{rad} I_a$ es un ideal primo y por tanto irreducible. Esto nos lleva a que $\operatorname{rad} I_a = \bigcap_{i \in \Lambda_a} \operatorname{rad} Q_i$ es en realidad $\operatorname{rad} I_a = \operatorname{rad} Q_i = P_i$, por tanto $J \subseteq \{P_1, P_2, \ldots, P_m\}$.

Por doble contenido llegamos a que $J = \{P_1, P_2, \ldots, P_m\}$ para cualquier descomposición primaria mínima de I. Y puesto que J depende solo de I y no de la descomposición que se haga de I tenemos que $\{P_1, P_2, \ldots, P_m\}$ es común a todas las descomposiciones primarias mínimas de I. ■

Definición. Si I es un ideal noetheriano de R entonces los ideales primos asociados a cualquiera de sus descomposiciones primarias reciben el nombre de **ideales primos asociados al ideal** I. Si un ideal primo asociado a I, P, no contiene a ningún otro ideal primo asociado a I entonces P se denomina **ideal primo aislado**. En caso contrario P se denomina **ideal primo encajado**.

Corolario 27. Sea Q un ideal propio de de un anillo R noetheriano. Un ideal primo P contiene a Q si y solo si P contiene a alguno de los primos asociados a Q.

Demostración:

Es fácil ver que si R es un anillo conmutativo, I y J ideales de R y P un ideal primo de R que contiene a IJ, o I o J estará contenido en P.

Sea ahora Q un ideal de R con descomposición primaria:

$$Q = Q_1 \cap \cdots \cap Q_n$$

En ese caso por la Proposición 15.(3)*:*

$$rad\, Q = rad\, Q_1 \cap \cdots \cap rad\, Q_n$$

Si P es un ideal primo que contiene a Q, por la Proposición 16*, P contiene a $rad\, Q$ o lo que es lo mismo:*

$$rad\, Q_1 \cap \cdots \cap rad\, Q_n \subseteq P$$

Por la observación del principio de la demostración, P contendrá a algún $rad\, Q_i$ es decir a algún primo asociado a Q. ■

Ejemplo:

Sea $I = (x^2, xy) \in \mathbb{R}[x, y]$. Entonces:

$$(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$$

son dos descomposiciones primarias mínimas de I. Entonces los primos asociados a I son (x) (porque al ser ideal primo es radical) y $rad\,((x, y)^2) = (x, y)$. Un ideal primo de $\mathbb{R}[x, y]$ contendrá a I si y solo si contiene a alguno de estos primos asociados. Sin embargo como (x, y) no es un primo aislado ya que $(x) \subseteq (x, y)$ se tiene que P contendrá a I si y solo si contiene a (x).

Notemos que (x), que es la componente primaria asociada al primo aislado, aparece en ambas descomposiciones.

3 Extensiones enteras y el teorema de ceros de Hilbert

3.1 Extensiones enteras

La extensiones enteras son la generalización del concepto de extensión algebraica a extensiones no necesariamente de cuerpos.

Definición. Supongamos que R es un subanillo de un anillo conmutativo S con $1 = 1_s \in R$

- Un elemento $s \in S$ es **entero** sobre R si s es la raíz de algún polinomio mónico de $R[x]$.
- El anillo S es una **extensión entera** de R si todo elemento de S es entero sobre R.
- La **clausura entera** de R en S es el conjunto de todos los elementos de S enteros sobre R.
- El anillo R se dice **íntegramente cerrado** en S si R coincide con su clausura entera en S
- La clausura entera del dominio de integridad R en su cuerpo de fracciones se denomina la **normalización** de R. R se dice **normal**(o **íntegramente cerrado** a secas) si es íntegramente cerrado en su cuerpo de fracciones.

Puede uno preguntarse por qué se exige la condición de que el polinomio del que un elemento entero es raíz sea mónico. Se exige está condición para que los elementos enteros posean propiedades muy similares a los algebraicos, como veremos a continuación. Obviamente, en polinomios sobre cuerpos, cualquier polinomio puede multiplicarse por una constante para hacerlo mónico. Por tanto sobre cuerpos, entero y algebraico son conceptos equivalentes.

Proposición 28. Sea R un subanillo del anillo conmutativo S con $1 = 1_S$ y sea $s \in S$. Entonces son equivalentes:

1. s es entero sobre R
2. $R[s]$ es un R-módulo finitamente generado (donde $R[s]$ es el anillo de todas las R-combinaciones lineales de s y sus potencias).
3. $s \in T$ para algún subanillo T, $R \subseteq T \subseteq S$, que es un R-módulo finitamente generado.

Demostración:

$\underline{1 \to 2}$ *Sea $s \in S$ raíz del polinomio $x^n + a_{n-1} + \cdots + a_0 \in R[x]$. En ese caso:*

$$s^n = -(a_{n-1}s^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0)$$

Luego s^n y por extensión todas las potencias posteriores de s pueden ser expresada como R-combinación lineal de $s^{n-1}, \ldots, s, 1$. Por tanto $R[s] = R + Rs + \cdots + Rs^{n-1}$ está finitamente generado como R-módulo.

$\underline{2 \to 3}$ *Coger* $R[s] = T$.

$\underline{3 \to 1}$ *Sea* T *el subanillo de* S *mencionado en* 3*, sea* $v_1, \ldots, v_n$ *su conjunto de generadores. Entonces para todo* $i \in \{1 \ldots, n\}$ $sv_i \in T$ *porque* T *es un anillo (luego está cerrado por productos). Entonces dicho* sv_i *puede ser escrito como:*

$$sv_i = \sum_{j=1}^{n} a_{ij} v_j$$

Pasando sv_i *a la derecha y aplicando la propiedad distributiva llegamos:*

$$0 = \sum_{j=1}^{n} (\delta_{ij} s - a_{ij}) v_j \qquad i = 1, 2, \ldots, n$$

donde δ *es la delta de Dirac. Sea* B *la matriz* $n \times n$ *con coeficientes* $b_{ij} = \delta_{ij} s - a_{ij}$ *y* v *es el vector* $n \times 1$ *con los* v_i*. Tenemos entonces la ecuación* $Bv = 0$*. Usando la regla de Cramer:*

$$v_i \det B = \det B_i$$

Siendo B_i *el resultado de resultado de sustituir la* i*-esima columna de* B *por el vector nulo. Esto implica que* $\det B_i = 0$*, luego* $v_i \det B = 0$ *para todo* i*. Como* $1 \in T$ *es* R*-combinación lineal de* $v_1, \ldots, v_n$*, multiplicando dicha combinación lineal por* $\det B$ *obtenemos que* $\det B = 0$*.* $B = Is - A$*,* A *siendo la matriz con los* $a_{ij} \in R$*. Por tanto la expresión de* $\det B$ *nos da un polinomio mónico de* $R[x]$ *del que* s *es raíz.*

■

Corolario 29. Sea R como en la proposición anterior y sea $s, t \in S$.

1. Si s y t son enteros sobre R entonces también lo son $s \pm t$ y st. La clausura entera de R en S es un subanillo de S que contiene a R.
2. El hecho de ser una extensión entera es transitivo. Sea $R \subseteq S \subseteq T$ anillos, si T es entero sobre S que es entero sobre R entonces T será entero sobre R.

Demostración:

$\underline{1.}$ *Sean* $s, t \in S$ *elementos enteros sobre* R*. Por la Proposición* 28.(2) $R[s]$ *y* $R[t]$ *están finitamente generados como* R*-módulos:*

$$R[s] = Rs_1 + Rs_2 + \cdots + Rs_n$$
$$R[t] = Rt_1 + Rt_2 + \cdots + Rt_m$$

Entonces

$$R[s,t] = Rs_1t_1 + \cdots + Rs_1t_m + Rs_2t_1 + \cdots + Rs_nt_m$$

es un anillo que contiene a $s + t$ *y a* st *y es finitamente generado como* R*-módulo (con* $n * m$ *generadores) por tanto por Proposición* 28.(3) *tenemos que* $s + t$ *y* st *son enteros sobre* R*.*

Como la clausura entera de R *en* S *es un subconjunto de* S *cerrado por sumas y productos será un subanillo. Que contiene a* R *es trivial.*

$\underline{2.}$ *Sea* $t \in T$*. Como* T *es entero sobre* S*,* t *será raíz de algún polinomio mónico* $p(x) \in S[x]$*.*

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in S[x]$$

Como cada $a_i \in S$ es entero sobre R cada anillo $R[a_i]$ está finitamente generado como R-módulo luego el anillo $R[a_1, \ldots, a_{n-1}]$ también estará finitamente generado como R-módulo.

$p(x) \in R[a_1, \ldots, a_{n-1}][x]$ es mónico y tiene a s como raíz, luego s es entero sobre $R[a_1, \ldots, a_{n-1}]$, por tanto $R[a_1, \ldots, a_{n-1}][s] = R[a_1, \ldots, a_{n-1}, s]$ está finitamente generado como $R[a_1, \ldots, a_{n-1}]$-módulo y por tanto también como R-módulo. Por la Proposición 28.(3), s es entero sobre R. ■

Una consecuencia inmediata del resultado (2) de este corolario es que la clausura entera de R en S es siempre íntegramente cerrada. Cualquier elemento en la clausura entera de la clausura entera de R es entero sobre R por tanto debe estar contenido en la clausura entera de R.

Ejemplos:

1. Si R y S son cuerpos entonces los enteros algebraicos de S sobre R son los elementos algebraicos de S sobre R. Esto se debe a que cualquier polinomio en $R[x]$ podemos dividirlo entre su coeficiente director para obtener un polinomio mónico con las mismas raíces.

2. Si S es una extensión entera de R e I es un ideal de S. Entonces S/I es una extensión entera de $R/(R \cap I)$. Solo hay que comprobar que si $s \in S$ es raíz de $p(x) \in R[x]$ mónico entonces $\overline{s} \in S/I$ es raíz de $\overline{p}(x) \in R/(R \cap I)[x]$. Notemos que por el segundo teorema de isomorfía del anexo, $(R + I)/I \cong R/(R \cap I)$, y así el polinomio $\overline{p}(x) \in (R + I)/I[x]$ se puede ver como un polinomio en $R/(R \cap I)[x]$.

3. Si R es dominio de factorización única, entonces R es normal (íntegramente cerrado en su cuerpo de fracciones). Sea a/b un elemento irreducible (a y b no tienen factores comunes) en el cuerpo de fracciones de R que es entero sobre R. Entonces:

   $$(a/b)^n + r_{n-1}(a/b)^{n-1} + \cdots + r_1(a/b) + r_0 = 0$$

   Operando:

   $$a^n = b(-r_{n-1}a^{n-1} - \cdots - r_1 a b^{n-2} - r_0 b^{n-1})$$

   Luego cualquier factor irreducible de b tendrá que dividir también a^n y por tanto a lo cual es una contradicción.

Definición. Sea $\varphi\colon R \to S$ un homomorfismo de anillos conmutativos.

1. Si I es un ideal de R, entonces la **extension** de I a S es el ideal $\varphi(I)S$, el ideal de S generado por la imagen de I.

2. Si J es un ideal de J, entonces la **contracción** en R de J es $\varphi^{-1}(J)$.

El propósito de esta definición es relacionar ideales de R y S a través de φ. La preimagen de un ideal por un homomorfismo es siempre un ideal así que la definición de contracción sale de manera natural. Sin embargo, la imagen de un ideal no es siempre un ideal, lo que se hace es coger el ideal más pequeño que contiene a la imagen.

Algunas propiedades muy básicas son:

1. $I \subseteq \varphi^{-1}(\varphi(I)) \subseteq \varphi^{-1}(\varphi(I)S)$, un ideal siempre está contenido en la contracción de su extensión.

2. $\varphi(\varphi^{-1}(J))S \subseteq J$, un ideal siempre contiene a la extensión de su contracción.

Aunque hemos dado la definición en general, en este trabajo solo usaremos el caso concreto en el que R es un subanillo de S y φ la inclusión natural. En este caso la extensión de I es IS y la contracción de J es $J \cap R$.

Teorema 30. Sea R un subanillo del anillo conmutativo S con $1 \in R$ y supongamos que S es entero sobre R.

1. Si S es un dominio de integridad, entonces R es un cuerpo si y solo si S es un cuerpo.

2. Sea P un ideal primo de R. Entonces existe un ideal primo Q en S con $P = Q \cap R$ (todo ideal primo de R es contracción de algún ideal primo de S). Es más, P es maximal si y solo si Q es maximal.

3. Sea $P_1 \subseteq P_2 \subseteq \ldots \subseteq P_n$ una cadena ascendente de ideales primos, $Q_1 \subseteq Q_2 \subseteq \ldots \subseteq Q_m$ una cadena de ideales primos de S con $P_i = Q_i \cap R$ (ideales de S que se contraen el los P_i), $1 \leq i \leq m$ y $m < n$. Entonces esta segunda cadena ascendente de ideales se puede completar. Es decir, existen ideales primos $Q_{m+1} \subseteq \cdots Q_n$ en S para los cuales $P_i = Q_i \cap R$ para todo i.

Demostración:

1. *Supongamos que R es un cuerpo y sea $s \in S$, $s \neq 0$. s es entero sobre R luego*

$$s^n + a_{n-1}s^{n-1} + \ldots a_1 s + a_0 = 0 \qquad a_{n-1} \ldots, a_0 \in R$$

Como S es dominio de integridad podemos asumir que $a_0 \neq 0$, en caso contrario $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s = 0$ luego $s(s^{n-1} + a_{n-1}s^{n-1} + \cdots + a_1) = 0$ y como S es dominio de integridad y $s \neq 0$ tendremos que $s^{n-1} + a_{n-1}s^{n-2} + a_1 = 0$. Si $a_1 = 0$ podríamos repetir el mismo razonamiento. Ahora:

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = -a_0$$

y como $-(1/a_0) \in R \subseteq S$

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1)(-1/a_0) = 1$$

$s^{n-1} + a^{n-1}s^{n-2} + \cdots + a_1)(-1/a_0) \in S$ es el inverso de s. Como esto se puede hacer para todo $s \in S$, S es un cuerpo.

Al revés, sea S es un cuerpo y $r \in R$, $R \neq 0$. $r^{-1} \in S$ luego será entero sobre R.

$$r^{-m} + a_{m-1}r^{-m+1} \cdots + a_1 r^{-1} + a_0 = 0 \quad a_{m-1}, \ldots, a_0 \in R$$

Entonces multiplicando todo por r^{m-1}

$$r^{-1} + a^{m-1} + a_{m-2}r + \cdots + a_1 r^{m-2} + a_0 r^{m-1} = 0$$
$$r^{-1} = -(a_{m-1} + a_{m-2}r + \cdots + a_1 r^{m-2} + a_0 r^{m-1}) \in R$$

2. *Solo probaremos ahora la segunda parte. Observemos que S/Q es extensión entera de R/P (por el ejemplo (2) anterior). Por (1) si S/Q es un cuerpo (Q es un ideal maximal) si y solo si R/P es un cuerpo (R es maximal).*

3. *Basta probar que si $P_1 \subseteq P_2$ ideales primos en R y Q_1 es un ideal primo en S tal que $P_1 = Q_1 \cap R$ entonces existe un ideal primo Q_2 en S tal que $P_2 = Q_2 \cap R$ y $Q_1 \subseteq Q_2$.*
Sea $\overline{S} = S/Q_1$ extensión entera de $\overline{R} = R/P_1$. La primera parte de (2) nos asegura que existe $\overline{Q_2}$ en $\overline{S}$ tal que $\overline{Q_2} \cap \overline{R} = P_2/P_1$. Entonces la preimagen Q_2 de $\overline{Q_2}$ en S es un ideal primo que contiene a P_2 tal que $Q_2 \cap R = P_2$. ■

Corolario 31. Supongamos que R es un subanillo del anillo S con $1_S \in R$ y asumamos que S es entero y finitamente generado (como anillo) sobre R. Si P es un ideal maximal en R, entonces hay un número finito no cero de ideales maximales Q en S tales que $Q \cap R = P$

Demostración:

Por el Teorema 30.(2) existe al menos un Q. Por tanto solo queda ver que existe un número finitos de Qs. Si Q es un ideal maximal de S con $Q \cap R = P$ entonces S/Q es un cuerpo que contiene al cuerpo R/P (S/Q contiene a $(R+Q)/Q$ que por el segundo teorema de isomorfía es isomorfo a $R/(Q \cap R) = R/P$).

Para ver que solo hay un número finito de Qs basta ver que solo hay un número finito de homomorfismos de S a un cuerpo que contenga a R/P y que extienda la proyección de R a R/P. Por hipótesis $S = R[s_1, \ldots, s_n]$ y cada s_i es entero sobre R, denotemos por $p_i(x)$ el polinomio mónico de $R[x]$ del que s_i es raíz. Si Q es un ideal maximal de S entonces $S/Q = R/P[\overline{s}_1, \ldots, \overline{s}_n]$ es la extensión de cuerpos sobre el cuerpo R/P con generadores $\overline{s}_1, \ldots, \overline{s}_n$. Además cada $\overline{s}_i$ es raíz del polinomio $\overline{p}_i(x)$ obtenido al proyectar los coeficientes de $p_i(x)$. Solo hay una cantidad finita de raíces de este polinomio (en una clausura algebraica fija de R/P) luego solo hay finitas posibles extensiones de cuerpos de la forma $R/P[\overline{s}_1, \ldots, \overline{s}_n]$, esto prueba el resultado. ■

3.2 El teorema de ceros de Hilbert

Con los resultados anteriores ya podemos probar un resultado de gran importancia para la geometría algebraica.

Definición. Si k es un cuerpo, los elementos $y_1, y_2, \ldots, y_n$ de alguna k-álgebra se dicen **algebraicamente independientes** sobre k si no existe ningún polinomio $p \in k[x_1, x_2, \ldots, x_n]$ para el cual $p(y_1, y_2, \ldots, y_n) = 0$.

Otra manera de ver la definición anterior es la siguiente: $y_1, \ldots, y_n$ son algebraicamente independientes si y solo si el homomorfismo:

$$\begin{array}{rccc} \phi\colon & k[x_1, \ldots, x_n] & \longrightarrow & k[y_1, \ldots, y_n] \\ & p(x_1, \ldots, x_n) & \longrightarrow & p(y_1, \ldots, y_n) \end{array}$$

es inyectivo.

Teorema 32. (*Lema de Normalización de Noether*) Sea k un cuerpo y supongamos que $A = k[r_1, r_2, \ldots, r_m]$ es una k-álgebra finitamente generada. Entonces para algún q, $0 \leq q \leq m$, existe un conjunto de elementos algebraicamente independientes $y_1, y_2, \ldots, y_q \in A$ de tal forma que A es entero sobre $k[y_1, y_2, \ldots, y_q]$.

Demostración:

Procedamos por inducción en m. El caso base si $m = 1$ es sencillo. Sea $A = k[r_1]$. Si $\{r_1\}$ es un conjunto algebraicamente independiente, entonces $k[r]$ es entero sobre si mismo y cumple todas la condiciones que describe el lema. Por otra parte si $\{r_1\}$ no es un conjunto algebraicamente independiente sobre k esto implicara que existe $p(x) \in k[x]$ tal que $p(r_1) = 0$. Esto quiere decir que $k[r_1]$ es algebraico sobre k y como k es un cuerpo, algebraico equivale a entero, asumimos que el conjunto vacío es por defecto algebraicamente independiente.

Ahora supongamos que el resultado se cumple para $m - 1$. Si $\{r_1, \ldots, r_m\}$ son elementos algebraicamente independientes sobre k entonces podemos coger $y_i = r_i$, $i = 1, \ldots, m$. Obviamente un anillo siempre es entero sobre si mismo.

En caso contrario existe $f \in k[x_1, \ldots, x_m]$ para el que $f(r_1, \ldots, r_m) = 0$. El polinomio f es una suma de monomios de la forma $cx_1^{e_1}x_2^{e_2}\ldots x_m^{e_m}$, siendo el grado del monomio $e_1 + \cdots + e_m$. Denotaremos como d al mayor grado de cualquier mónomio de f. Reordenando la variables si es necesario podemos asumir que f es un polinomio no constante para la variable x_m con coeficientes $k[x_1, \ldots, x_{m-1}]$.

Realizaremos un cambio de variable para transformar f en un polinomio mónico en x_m con coeficientes en un subanillo de A generado sobre k por $m - 1$ elementos.

Definamos los enteros $\alpha_i = (1 + d)^i$ y nuevas variables $X_i = x_i - x_m^{\alpha_i}$ para $1 \leq i \leq m - 1$. Sea:

$$g(X_1, \ldots, X_{m-1}, x_m) = f(X_1 + x_m^{\alpha_1}, \ldots, X_{m-1} + x^{\alpha_{m-1}}, x_m)$$

Entonces $g \in k[X_1, \ldots, X_{m-1}, x_m]$. Cada término monomial de f contribuirá a g con un solo término de la forma cx_m^e con c constante. Además debido a la elección de los α_i el valor de e será distinto para cada monomio. Aclaremos esto último, un monomio de $g = f(X_1 + x_m^{\alpha_1}, \ldots, X_{m-1} + x_m^{\alpha_{m-1}}, x_m)$ tendrá la forma:

$$c(X_1 + x_m^{\alpha_1})^{e_1} \ldots (X_{m-1} + x_m^{\alpha_{m-1}})^{e_{m-1}} x_m^{e_m}$$

Operando podemos separar un término de la forma:

$$cx_m^{e_1\alpha_1 + \cdots + \alpha_{m-1}e_{m-1} + e_m}$$

Donde

$$e_1\alpha_1 + \cdots + \alpha_{m-1}e_{m-1} + e_m = e$$

Como por definición de d, $e_i \leq d < 1 + d$ y $\alpha_i = (1 + d)^i$, e es la expresión de un número entero en base $1 + d$ ($e_m = e_m(1 + d)^0$) luego el e que aporta cada monomio será distinto. En caso contrario habría dos monomios con el mismo multigrado lo cual es imposible, los simplificaríamos sumándolos.

Definamos N como el mayor grado de x_m para cualquier monomio de g, tendremos que:

$$g = ax_m^N + \sum_{i=0}^{N-1} h_i(X_1, \ldots, X_{m-1})x_m^i$$

Para algún $c \in k$ distinto de cero. Si ahora cogemos $s_i = r_i - r_m^{\alpha_i}$ tendremos que

$$\frac{1}{c}g(s_1, s_2, \ldots, s_{m-1}, r_m) = \frac{1}{c}f(r_1, r_2, \ldots, r_{m-1}, r_m) = 0$$

Lo que nos dice que r_m es entero sobre $B = k[s_1, \ldots, s_{m-1}]$. Por otro lado cada r_i será algebraico sobre $B[r_m]$ ya que r_i es raíz del polinomio $x - s_i - r_m^{\alpha_i}$. Por tanto A es entero sobre $B[r_m]$ y como ser entero es transitivo (Corolario 29.(2)), A es entero sobre B.

B es una k-álgebra generada por $m-1$ elementos luego por hipótesis de inducción será algebraica sobre un $k[y_1, \ldots, y_q]$ $0 \leq q \leq m_1$ con $\{y_1, \ldots, y_{m-1}\}$ algebraicamente independientes. Aplicando otra vez que ser entero es transitivo tendremos que A también es entero sobre $k[y_1, \ldots, y_q]$ probando el resultado.

■

Ya estamos en posición de demostrar el teorema de ceros de Hilbert.

Teorema 33. (*Teorema de ceros de Hilbert, forma débil*). Sea k un cuerpo algebraicamente cerrado. Entonces M es un ideal maximal en el anillo de polinomios $k[x_1, x_2, \ldots, x_n]$ si y solo si $M = (x_1 - a_1, \ldots, x_n - a_n)$ para ciertos $a_1, a_2, \ldots, a_n \in k$. Esto equivale a decir que las aplicaciones $\mathcal{Z}$ e $\mathcal{I}$ definen una correspondencia biyectiva:

$$\{ \text{ puntos de } \mathbb{A}^n \} \quad \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \quad \{ \text{ ideales maximales de } k[\mathbb{A}^n] \}$$

En concreto, si I es un ideal propio de $k[x_1, x_2, \ldots, x_n]$ entonces $\mathcal{Z}(I) \neq \emptyset$.

Demostración:

Ya sabemos que $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal maximal de $k[x_1, \ldots, x_n]$ luego solo queda probar el recíproco.

Sea M un ideal maximal cualquiera de $k[x_1, \ldots, x_n]$ y sea $E = k[x_1, \ldots, x_n]/M$. E es un cuerpo que contiene a k y esta finitamente generado sobre dicho k (por $\overline{x}_1, \ldots, \overline{x}_n$). Por el Lema de Normalización de Noether, E es entero sobre algún anillo de polinomios $k[y_1, \ldots, y_q]$. Por el Teorema 30.(1) $k[y_1, \ldots, y_q]$ es un cuerpo, pero un anillo de polinomios en una o más variables nunca es un cuerpo luego necesariamente tenemos que $q = 0$, $k[y_1, \ldots, y_q] = k$. E es entero sobre k, luego al ser k cuerpo esto equivale a que E es algebraico sobre k. Sin embargo por hipótesis sabemos que k es algebraicamente cerrado luego $E = k$, es decir, para cada $\overline{x}_i$ que genera E, $\overline{x}_i \in k$ $1 \leq i \leq n$. Esto implica que para cada $i = 1, \ldots, n$ existe un $a_i \in k$ tal que $x_i - a_i \in M$. Esto nos dice que el ideal $(x_1 - a_1, \ldots, x_n - a_n)$ está contenido en M. Dicho ideal es maximal luego $M = (x_1 - a_1, \ldots, x_n - a_n)$.
Por último si I es un ideal propio no nulo de $k[x_1, \ldots, x_n]$, I está contenido en un ideal maximal $(x_1 - a_1, \ldots, x_n - a_n)$, luego $\mathcal{Z}((x_1 - a_1, \ldots, x_n - a_n)) = (a_1, \ldots, a_n) \in \mathcal{Z}(I)$. ■

Teorema 34. (*Teorema de ceros de Hilbert*) Sea k un cuerpo algebraicamente cerrado. Entonces $\mathcal{I}(\mathcal{Z}(I)) = rad\, I$ para cada ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$. Es más, las aplicaciones $\mathcal{Z}$ e $\mathcal{I}$ definen una correspondencia biyectiva:

$$\{ \text{ conjuntos algebraicos afines } \} \quad \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \quad \{ \text{ ideales radicales } \}$$

Demostración:

Que $rad\, I \subseteq (\mathcal{I}(\mathcal{Z}(I))$ es fácil así que solo probaremos el otro contenido. Por el teorema de bases de Hilbert $k[x_1, \ldots, x_n]$ es noetheriano luego $I = (f_1, f_2, \ldots, f_m)$ está finitamente generado. Sea $g \in \mathcal{I}(\mathcal{Z}(I))$. Introduzcamos una nueva variable x_{n+1} y definamos el ideal $I' = (f_1, \ldots, f_m, x_{n+1}g - 1) \subseteq k[x_1, \ldots, x_n, x_{n+1}]$. En cualquier punto de $\mathbb{A}^{n+1}$ donde $f_1, \ldots, f_m$ se anulen, g también se anulará pues $g \in \mathcal{I}(\mathcal{Z}(I))$ luego $x_{n+1}g - 1$ NO se anulara. Por tanto $\mathcal{Z}(I') = \emptyset$ en $\mathbb{A}^{n+1}$. Por la forma débil del teorema de ceros de Hilbert I' no puede ser un ideal propio, o lo que es lo mismo, $1 \in I'$. Sea:

$$1 = a_1 f_1 + \cdots + a_m f_m + a_{m+1}(x_{n+1}g - 1) \quad \textit{para } a_i \in k[x_1, \ldots, x_{n+1}] \textit{ con } i = 1, \ldots, m+1$$

Definiendo $y = 1/x_{n+1}$ y multiplicando la ecuación anterior por una potencia lo suficientemente grande de y, N, tenemos que:

$$y^N = c_1 f_1 + \cdots + c_m f_m + c_{m+1}(g - y) \quad \textit{para algún } c_i \in k[x_1, \ldots, x_n, y]$$

Sustituyendo g por y en esta ecuación polinómica muestra que $g^N \in I$, es decir, $g \in rad\, I$. Luego $\mathcal{I}(\mathcal{Z}(I)) \subseteq rad\, I$ y $\mathcal{I}(\mathcal{Z}(I)) = rad\, I$ como queríamos probar.

■

Además también tenemos una generalización de teorema de ceros de Hilbert para cuando k no es algebraicamente cerrado.

Corolario 35. Si k es un cuerpo con clausura algebraica $\overline{k}$ e I es un ideal de $k[x_1, \ldots, x_n]$, entonces $\mathcal{I}_k(\mathcal{Z}_{\overline{k}}(I)) = rad\, I$, siendo $\mathcal{Z}_{\overline{k}}(I)$ el conjunto de raíces en $\overline{k}^n$ de los polinomios de I y $\mathcal{I}_k(\mathcal{Z}_{\overline{k}}(I)) = rad\, I$ es el ideal de los polinomios de $k[x_1, x_2, \ldots, x_n]$ que se anulan en todos los puntos de $\mathcal{Z}_{\overline{k}}(I)$.

La importancia del teorema de ceros de Hilbert reside en que nos permite relacionar elementos geométricos con elementos algebraicos.

Geometría	**Algebra**
conjuntos algebraicos afines	Anillos de coordenadas $k[V]$
Puntos en V	Ideales maximales en $k[V]$
Subconjuntos algebraicos de V	Ideales radicales de $k[V]$
Subvariedades de V	Ideales primos en $k[V]$
morfismos $\varphi\colon V \to W$	Homomorfismos de k-álgebras $\widetilde{\varphi}\colon k[W] \to k[V]$

Estas relaciones se pueden establecer también para cualquier conjunto algebraico V y no solo para $\mathbb{A}^n$ usando el cuarto teorema de isomorfia. Por ejemplo, cada punto $v \in V$ tiene asociado un único ideal maximal de $k[\mathbb{A}^n]$ a través de $\mathcal{I}$. Además vimos que si $A \subseteq B$ entonces $\mathcal{I}(B) \subseteq \mathcal{I}(A)$, por tanto $\mathcal{I}(V) \subseteq \mathcal{I}(v)$ y aplicando el cuarto teorema de isomorfia a $\mathcal{I}(v)$ le corresponde un único ideal maximal en $k[V] = k[\mathbb{A}^n]/\mathcal{I}(V)$, todo el resto de generalizaciones son idénticas.

Cálculo de radicales

Vemos algunos métodos básicos para calcular radicales. Existen métodos más complejos pero no los veremos en este trabajo.

Para empezar hay un caso que es sencillo, para $I = (f)$ con $f \in k[x_1, \ldots, x_n]$, como $k[x_1, \ldots, x_n]$ es un dominio de factorización única, podemos factorizar $f = p_1^{a_1} \ldots p_s^{a_s}$ luego $rad\,(f) = (p_1, \ldots, p_s)$.

Para casos más generales damos el siguiente criterio.

Proposición 36. Supongamos que k es un cuerpo. Si $I = (f_1, \ldots, f_s)$ es un ideal propio de $k[x_1, \ldots, x_n]$, entonces $f \in rad\, I$ si y solo si $(f_1, \ldots, f_s, 1 - yf) = k[x_1, \ldots, x_n, y]$.

Demostración:

$(f_1, \ldots, f_s, 1 - yf) = k[x_1, \ldots, x_n, y]$ *si y solo si*

$$1 - yf(x_1, \ldots, x_n), f_1(x_1, \ldots, x_n), \ldots, f_s(x_1, \ldots, x_n)$$

No tiene ceros comunes en la clausura algebraica $\overline{k}$ *de* k. *Dado* $(a_1, \ldots, a_n) \in \overline{k}^n$, $1 - yf(a_1, \ldots, a_n) = 0$ *tiene solución salvo que* $f(a_1, \ldots, a_n) = 0$. *Luego el sitema tiene ceros comunes salvo que en los puntos que* $f_1(a_1, \ldots, a_n) = \cdots = f_s(a_1, \ldots, a_n) = 0$ *también suceda que* $f(a_1, \ldots, a_n) = 0$. *Es decir si y solo si* $f \in \mathcal{I}_k(\mathcal{Z}_{\overline{k}}(I)) = rad\, I$ *por el Corolario* 35. ∎

Combinando este criterio con el hecho de que las bases de Gröbner reducidas son únicas obtenemos un método para comprobar si un polinomio se encuentra en el radical de un ideal.

Corolario 37. Supongamos $I = (f_1, \ldots, f_s)$ en $k[x_1, \ldots, x_n]$. Entonces $f \in rad\, I$ si y solo si $\{1\}$ es la base reducida de Gröbner del ideal $(f_1, \ldots, f_s, 1 - yf) \subseteq k[x_1, \ldots, x_n, y]$ respecto a un orden monomial cualquiera.

Entonces para comprobar que $f \in rad\, I$ usamos el algoritmo de Buchberger para calcular la base reducida de Gröbner de $(f_1, \ldots, f_s, 1 - yf)$ y comprobar si es $\{1\}$.

Ejemplo:

Sea el ideal $I = (x^3 + y^3 + z^3, x^2 + y^2 + z^2, (x + y + z)^3) \subset k[x, y, z]$. Veamos si $x \in rad\, I$. Para ello calculamos la base de Gröbner reducida del ideal $I' = (x^3 + y^3 + z^3, x^2 + y^2 + z^2, (x + y + z)^3, 1 - xv) \subseteq k[x, y, z, v]$. Efectivamente es 1 luego $I' = k[x, y, z, v]$ y $x \in rad\, I$. Se comprueba de la misma manera que $y, z \in rad\, I$ luego $rad\, I = k[x, y, z]$.

3.3 Anexo: Enteros Algebraicos

En esta parte vamos a concretar los resultados de 3.1 al caso concreto de extensiones del anillo $\mathbb{Z}$.

Definición. Sea K un cuerpo extensión de $\mathbb{Q}$.

- Un elemento $\alpha \in K$ se denomina **entero algebraico** si α es entero sobre $\mathbb{Z}$. Es decir, si α es raíz de algún polinomio mónico en $\mathbb{Z}[x]$.
- La clausura integral de $\mathbb{Z}$ en K se denomina **anillo de enteros** de K, denotado $\mathcal{O}_K$.

Fijémonos que como $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$, cualquier cuerpo que contenga a $\mathbb{Z}$ debe contener a $\mathbb{Q}$ necesariamente. Además es obvio que si α es entero sobre $\mathbb{Z}$ también lo será sobre $\mathbb{Q}$ aunque no al revés (basta coger $3/5$ como un contraejemplo cualquiera).

Nuestro primer resultado ahora será uno que nos ayude a comprobar cuando un elemento α es un entero algebraico.

Proposición. Un elemento α contenido en algún cuerpo extensión de $\mathbb{Q}$ es un entero algebraico si y solo si α es algebraico sobre $\mathbb{Q}$ y su polinomio mínimo $m_{\alpha,\mathbb{Q}}(x)$ tiene coeficientes enteros. En particular, los enteros algebraicos de $\mathbb{Q}$ son los enteros, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Para distinguir a los enteros de $\mathbb{Z}$ de todos los demás enteros algebraicos en este contexto usaremos el término *enteros racionales* para referirnos a ellos (porque son los enteros algebraicos de los números racionales). Ahora lo único que daremos son algunas propiedades de $\mathcal{O}_K$.

Teorema. Sea K un cuerpo extensión algebraica de $\mathbb{Q}$ de grado n.

1. El anillo de enteros $\mathcal{O}_k$ en K es noetheriano y es un $\mathbb{Z}$-módulo de rango n.
2. Para cada $\beta \in K$ existe algún $d \in \mathbb{Z}$ no nulo para el cual $d\beta$ es un entero algebraico. En particular, K es el cuerpo de fracciones de $\mathcal{O}_K$.
3. Si $\beta_1, \beta_2, \ldots, \beta_n$ es una $\mathbb{Q}$-base de K, entonces existe un entero d tal que $d\beta_1, d\beta_2, \ldots, d\beta_n$ es una base de un $\mathbb{Z}$-submódulo libre de $\mathbb{O}_K$ de rango n. Cualquier base de $\mathcal{O}_K$ es también una base de K como espacio vectorial sobre $\mathbb{Q}$.

Definición. Una **base entera** de la extensión algebraica K de $\mathbb{Q}$ es una base de su anillo de enteros en K considerada como un $\mathbb{Z}$-módulo de rango $[K : \mathbb{Q}]$.

4 Localización

4.1 Localización respecto a un subconjunto cerrado para multiplicación

La localización especialmente la localización en un primo es una técnica algebraica muy útil para estudiar el comportamiento de ideales dentro de un anillo.

Lo primero que hacemos es definir una generalización del concepto de anillo de fracciones sobre anillos que no sean necesariamente dominios de integridad. Sea R un anillo unitario y sea D un subconjunto de R cerrado por multiplicación que contiene a 1. Buscamos construir $D^{-1}R$, el menor anillo en el que todos los elementos de D son invertibles.

La mayor diferencia con respecto a los anillos de fracciones usuales es que ahora permitimos divisores de cero como denominadores. Como consecuencia estos $D^{-1}R$ no tendrá porque tener a R como subanillo. Esto hace todos los conceptos bastante menos intuitivos.

Teorema 38. Sea R un anillo conmutativo con $1 \neq 0$ y sea D un subconjunto de R cerrado por productos con $1 \in D$. Entonces existe:

- Un anillo conmutativo $D^{-1}R$
- Un homomorfismo de anillos $\pi\colon R \to D^{-1}R$

Entre los dos satisfacen la siguiente propiedad:
Para todo homomorfismo $\psi\colon R \to S$ de anillos conmutativos que envía 1_R a 1_S y para el cual $\psi(d)$ es invertible en S para todo d contenido en D, existe un único homomorfismo $\Psi\colon D^{-1} \to R$ tal que $\Psi \circ \pi = \psi$.

Demostración:

Está demostración es un análogo a la de la construcción de anillos de fracciones usual pero es constructiva así que es interesante verla.

Empezamos cogiendo el producto cartesiano $R \times D$ y definimos la siguiente relación de equivalencia en él:

$$(r_1, d_1) \sim (r_2, d_2) \text{ si y solo si } \quad x(d_2r_1 - d_1r_2) = 0 \quad \text{para algún } x \in D$$

Es fácil demostrar que efectivamente es una relación de equivalencia, las propiedad reflexiva y simétrica son inmediatas. Para la transitividad supongamos que $(r_1, d_1) \sim (r_2, d_2)$ y $(r_2, d_2) \sim (r_3, d_3)$, es decir $x(d_2r_1 - d_1r_2) = y(d_3r_2 - d_2r_1) = 0$ con $x, y \in D$. Entonces multiplicando por d_3, d_1 respectivamente y sumándolos

$$d_3yx(d_2a_1 - d_1a_2) = 0 \qquad d_1xy(d_3a_2 - d_2a_3) = 0$$
$$xy(d_3d_2a_1 - \underline{d_3d_1a_2} + \underline{d_1d_3a_2} - d_1d_2a_3) = 0$$
$$d_2yx(d_3a_1 - d_1a_3) = 0$$

Como $d_2, x, y \in D$ que es cerrado por productos, entonces $d_2xy \in D$.

Denotemos como r/d a la clase de equivalencia de (r, d) por $\sim$ y $D^{-1}R$ el conjunto de todas las clases de equivalencia. Definimos la suma y multiplicación en $D^{-1}R$:

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} = \frac{r_1d_2 + r_2d_1}{d_1d_2} \qquad \frac{r_1}{d_1} \times \frac{r_2}{d_2} = \frac{r_1r_2}{d_1d_2}$$

Comprobar que estas operaciones están bien definidas y dan estructura de anillo conmutativo y unitario (con unidad $1/1$) a $D^{-1}R$ es un ejercicio de cuentas sencillo.

Notemos que con está definición, para cada $d \in D$, $d/1$ es invertible en $D^{-1}R$. Esto no quiere decir d sea invertible en $D^{-1}R$, porque D no está necesariamente contenido en $D^{-1}R$ (algunos elementos pueden colapsar en las clases de equivalencia).

Finalmente definimos $\pi\colon R \to D^{-1}R$ con $\pi(r) = r/1$. Comprobar que π es un homomorfismo de anillos es sencillo. Supongamos ahora que $\psi\colon R \to S$ es un homomorfismo de anillos tal que $\psi(1_R) = 1_S$ y $\psi(d)$ es una unidad de S para todo $d \in D$. Definimos:

$$\begin{array}{rccl} \Psi\colon & D^{-1}R & \to & S \\ & \frac{r}{d} & \to & \Psi(\frac{r}{d}) = \psi(r)\psi(d)^{-1} \end{array}$$

Ψ está bien definido, si $r_1/d_1 = r_2/d_2$ esto es porque $x(d_2r_1 - d_1r_2) = 0$ para algún $x \in D$. Entonces $\psi(x)(\psi(d_2r_1) - \psi(d_1r_2)) = 0$ en S y ya que $\psi(x)$ es invertible de S no puede ser un divisor de 0. Por tanto $\psi(r_1)\psi(d_1)^{-1} = \psi(r_2)\psi(d_2)^{-1}$. Que $\Psi \circ \pi = \psi$ es inmediato.

Ya solo queda probar que Ψ es único. Primero observemos que todo elemento $r/d \in D^{-1}R$ puede ser expresado como $(r/1)(d/1)^{-1}$. Para elementos de la forma $x/1$ tenemos que $\Psi(x/1) = \Psi(\pi(x)) = \psi(x)$ únicamente determinado. Como Ψ es un homomorfismos de anillos, si está determinado $\Psi(u)$ también estará determinado $\Psi(u^{-1})$. Luego ψ es único. ∎

Dentro de $D^{-1}R$ podremos referirnos a $\pi(r) = r/1$, $r \in R$ usando sencillamente r.

Corolario 39. En la notación del teorema anterior.

1. $ker\,\pi = \{r \in R \mid xr = 0 \text{ para algún } x \in D\}$. En particular, $\pi\colon R \to D^{-1}R$ es inyectiva si y solo si D no contiene a cero ni a ningún divisor de cero en R.
2. $D^{-1}R = 0$ si y solo si $0 \in D$ o lo que es lo mismo, si D contiene elementos nilpotentes.

Observemos que si R es un dominio de integridad, cada $D^{-1}R$ será un subanillo del cuerpo fracciones de R. Esto se debe a que dado $(r_1, d_1), (r_2, d_2) \in R \times D$, al no haber divisores de cero $x(d_2r_1 - r2, d_1r_2) = 0$ solo se pueden dar dos casos:

- $0 = x \in D$ en cuyo caso hemos visto que $D^{-1}R = 0$ trivial.
- $d_2r_1 - d_1r_2 = 0$ que no depende del D que hayamos elegido. Luego ambas tuplas siempre pertenecerán a la misma clase de equivalencia da igual el D que hayamos elegido.

Por tanto cuando trabajemos con dominios de integridad si $(r_1, d_1) \sim (r_2, d_2)$ en $D^{-1}R$ esto se respetara en cualquier otro $J^{-1}R$ siempre que este no sea trivial y que $d_1, d_2 \in J$.

Definición. El anillo $D^{-1}R$ recibe el nombre de **anillo de fracciones** de R con respecto a D o la **localización** de R en D

Ejemplos:

- Si R es un dominio de integridad y $D = R - \{0\}$. Entonces $D^{-1}R$ es el cuerpo de fracciones de R.
- Sea P es un ideal primo en cualquier anillo R y sea $D = R - P$. Por definición de ideal primo, D es cerrado por multiplicación. Pasar al anillo $D^{-1}R$ se dice **localizar** R en P y el anillo se suele denotar R_P
- Por ejemplo, si $R = \mathbb{Z}$ y $P = (p)$ es un ideal primo, entonces

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\} \subset \mathbb{Q}$$

A continuación estudiaremos las extensiones y contracciones de ideales con respecto al homomorfismo π tal como las definimos en la sección tres. Para simplificar la notación la extensión de un ideal I la denotaremos ${}^cI$ y la contracción ${}^eI$.

Si I es un ideal de R, es fácil ver que todo elemento de ${}^eI$ se podrá expresar de la forma a/d con $a \in I$ y $d \in D$. Debido a esto a veces denotamos ${}^eI$ como $D^{-1}I$. Por la misma definición de extensión $D^{-1}I$ es un ideal de $D^{-1}R$.

Proposición 40. Con la notación que hemos establecido antes.

1. Para cualquier ideal J de $D^{-1}R$ tenemos que $J = {}^e({}^cJ)$. En particular, todo ideal de $D^{-1}R$ es una extensión de algún ideal de R, y distintos ideales de $D^{-1}R$ tienen distintas contracciones en R.
2. Para cualquier ideal I de R tenemos que:

$$ {}^c({}^eI) = \{r \in R \mid dr \in I \text{ para algún } d \in D\}$$

   En concreto, ${}^eI = D^{-1}R$ si y solo si $I \cap D \neq \emptyset$.

3. Extensiones y contracciones dan las correspondencias biyectivas:

Ideales primos P en R con $P \cap D = \emptyset$	$\xrightarrow{e}$ $\xleftarrow[c]{}$	Ideales primos de $D^{-1}R$

4. Si R es un anillo noetheriano entonces $D^{-1}R$ es noetheriano también.

Demostración:

1. *Ya vimos en la sección 3 que siempre se cumple que ${}^e({}^cJ) \subseteq J$ luego solo tenemos que ver el inverso. Sea $a/d \in J$. Entonces $a/1 = d(a/d) \in J$, luego $a \in \pi^{-1}(J) = {}^cJ$. Luego $a/1 \in {}^e({}^cJ)$, en ese caso como ${}^e({}^cJ)$ es un ideal $(a/1)(1/d) = a/d \in {}^e({}^cJ)$ probando que $J \subseteq {}^e({}^cJ)$ y por tanto $J \subseteq {}^e({}^cJ)$. Las demás afirmaciones de este apartado son inmediatas.*

2. *Sea $I' = \{r \in R \,|\, dr \in I \text{ para algún } d \in D\}$. Primero veamos que $I' \subseteq {}^c({}^eI)$. Si $r \in I'$ entonces existe algún $d \in D$ para el que $dr = a \in I$. En ese caso $r/1 = a/d \in {}^eI$, luego $r \in {}^c({}^eI)$. Ahora ${}^c({}^eI) \subseteq I'$. Sea $r \in {}^c({}^eI)$, $r/1 = a/d \in {}^eI$ $(a \in I, d \in D)$. Existe $x \in D$ tal que $x(dr - a) = 0$, $xdr = xa \in I$ y como $xd \in D$ tendremos que $r \in I'$. Por tanto ${}^c({}^eI) \subseteq I'$ y ${}^c({}^eI) = I'$*

Para la segunda afirmación ${}^eI = D^{-1}R$ *si y solo si* $1 \in {}^c({}^eI) = I'$ *(*$1/1 \in {}^eI$*). Esto solo ocurre si existe* $d \in D$ *tal que* $d1 = d \in I$*, es decir, si* $D \cap I \neq \emptyset$*.*

3. *Observemos primero que si* Q *es un ideal primo de* $D^{-1}R$ *entonces su preimagen por* π*,* ${}^cQ$*, es un ideal primo. Por tanto contraer lleva ideales primos de* $D^{-1}R$ *a ideales primos de* R *disjuntos de* D *(si* $\pi^{-1}(Q) \cap D \neq \emptyset$ *y tendremos que* ${}^e({}^cQ) = Q = D^{-1}R$*). Al revés, sea* P *un ideal primo de* R *disjunto de* D *y sea* $Q = {}^eP$*. Supongamos que* $(a/d_1)(b/d_2) \in Q$*, entonces* $ab/(d_1d_2) = c/d$ *con* $c \in P$ *y* $d \in D$*. Luego* $x(abd - cd_1d_2) = 0$ *para algún* $x \in D$*. Como* $c \in P$ *tenemos que* $xdab \in P$ *y como* P *es primo disjunto de* D *y* $xd \in D$*, necesariamente* $ab \in P$ *y otra vez como* P *es primo tenemos que* a *o* b *está en* P*. Por tanto* $a/d_1 \in Q$ *o* $b/d_2 \in Q$*, es decir* Q *es primo en* $D^{-1}R$*.*

Ahora solo queda ver que en este caso la inversa de la contracción es la extensión (que es precisamente el apartado (1) *y que la inversa de la extensión es la contracción. Por* (2)*:*

$$^c({}^eI) = \{r \in R \,|\, dr \in P \text{ con } d \in D\}$$

Como P *es primo disjunto de* D*,*$r \in {}^e({}^cP)$ *si y solo si* $dr \in P$*, lo que implica que* d *o* r *estará en* P *y como* d *no es porque está en* D *tendrá que ser* $r \in R$*.* ${}^e({}^cP) = P$*.*

4. *Por la última afirmación* (1) *toda cadena ascendente de ideales en* $D^{-1}R$ *induce una única cadena ascendente de ideales en* R *(sus contracciones).* ■

Definición. Supongamos que R es un anillo conmutativo unitario y D un subconjunto cerrado por multiplicación que contiene al 1. La **saturación** del ideal I en R con respecto a D es el ideal ${}^c({}^eI)$ en R calculando la extensión y contracción con respecto a π. Si $I = {}^c({}^eI)$ entonces I se dice **saturado** con respecto a D.

Fijándonos en el apartado (2) de la Proposición 40 la saturación de un ideal I puede definirse de manera informal como los elementos en R que estarían en D si pudiésemos multiplicar por denominadores de D. El ideal es saturado si no obtuviéramos ningún elemento nuevo de esa forma.

4.2 Determinar si un ideal en $k[x_1, x_2, \ldots, x_n]$ es primo

Sea P un ideal en el anillo de polinomios de $k[x_1, \ldots, x_n]$. Si P es primo, entonces cada $P_i = P \cap k[x_1, \ldots, x_i]$ $0 \leq i \leq n$ será ideal primo en su respectivo $k[x_1, \ldots, x_i]$. Si somos capaces de comprobar cuándo un ideal I de un anillo $R[x]$ es primo sabiendo que $I \cap R$ es primo en R, entonces solo necesitaremos comprobar que P_0 es un ideal primo de k y usar que $k[x_1, \ldots, x_i] = k[x_1, \ldots, x_{i-1}][x_i]$, para ir comprobando que cada P_i es primo a partir de P_{i-1} hasta llegar a $P_n = P$.

Sea R un anillo conmutativo y P un ideal primo de $R[x]$, entonces $P \cap R$ es un ideal primo de R luego $S = R/(P \cap R)$ es un dominio de integridad. Por último sea F el cuerpo de fracciones de S. Tenemos pues dos homomorfismos que surgen de manera natural, la proyección de $R[x]$ en $(R/P \cap R)[x]$ y la inclusión de $S[x]$ en $F[x]$, que denotaremos p e i respectivamente:

$$R[x] \xrightarrow{p} (R/P \cap R)[x] = S[x] \xrightarrow{i} F[x]$$

Recordemos que en este caso F se puede considerar como la localización del dominio de integridad S respecto al conjunto $S - \{\overline{0}\}$.

Proposición 41. Supongamos que R es un anillo conmutativo y unitario y que I es un ideal de $R[x]$. Con la notación anterior I es un ideal primo en $R[x]$ si y solo si

1. $J = I \cap R$ es un ideal primo en R (o lo que es lo mismo $S = R/J$ es un dominio de integridad).
2. Siendo $\overline{I}$ es la imagen de I en $S[x]$, $\overline{I}F[x]$ es un ideal primo en $F[x]$ que satisface que $\overline{I}F[x] \cap S[x] = \overline{I}$ ($\overline{I}$ es un ideal saturado).

Demostración:

Supongamos que I es un ideal primo en $R[x]$, luego $J = I \cap R$ es un ideal primo en R y $S = R/J$ es un dominio integridad. El núcleo de:

$$\begin{array}{rccc} p\colon & R[x] & \longrightarrow & S[x] = (R/J)[x] \\ & x & \longrightarrow & x \\ & r & \longrightarrow & \overline{r} \end{array}$$

es $J[x]$ y $J[x] \subseteq I$.

Sea $\psi\colon A \to B$ un homomorfismo suprayectivo de anillos y D un ideal de A tal que $\ker\psi \subseteq D$. Ahora sea:

$$\begin{array}{rccc} \psi_D\colon & A & \longrightarrow & B/\psi(D) \\ & a & \longrightarrow & \overline{\psi(a)} \end{array}$$

Como ψ es suprayectiva ψ_D también lo será porque es la composición de dos aplicaciones suprayectivas: ψ y la proyección de B en $B/\psi(D)$.

Veamos que $\ker\psi_D = D$. $\psi_D(a) = 0$ si y solo si $\psi(a) \in \psi(D)$ o sea $\ker\psi_D = \psi^{-1}(\psi(D)) \supseteq D$. Cojamos $r \in \ker\psi_D$, como $\psi(r) \in \psi(D)$ existe $d \in D$ tal que $\psi(r) = \psi(d)$, $\psi(r) - \psi(d) = 0$. Por ser ψ homomorfismo de anillos $\psi(r-d) = 0$, es decir $r - d \in \ker\psi$, pero $\ker\psi \subseteq D$ luego $r - d = c \in D$, $r = c + d \in D$. Como $c, d \in D$ tenemos que $r \in D$ luego $\ker\psi_D \subseteq D$ y por doble contenido $\ker\psi_D = D$. Aplicando el primer teorema de isomorfía vemos que $A/D \cong B/\psi(D)$.

Aplicando esto a $p\colon R[x] \to S[x]$ e I (que contiene a $J[x] = \ker(p)$) obtenemos que $R[x]/I \cong S[x]/\overline{I}$ (recordemos que $\overline{I}$ es la imagen de I por p).

Ahora como I es primo $R[x]/I$ es un dominio de integridad luego $S[x]/\overline{I}$ también lo será, lo que solo ocurre si $\overline{I}$ es un ideal primo de $S[x]$.

Los elementos de $\overline{I} \cap S$ son las imágenes de los elementos de $I \cap R$ por p y $I \cap R = \ker p$ luego $\overline{I} \cap S = 0$. Como $F[x]$ es la localización de $S[x]$ respecto a $D = S - \{0\}$, por la Proposición 40.(3) $\overline{I}$ es un ideal primo de $S[x]$ tal que $\overline{I} \cap D = \emptyset$, por tanto ${}^e\overline{I} = \overline{I}F[x]$ es primo, y por la Proposición 40.(1) $\overline{I} = {}^c({}^e\overline{I}) = \overline{I}F[x] \cap S[x] = \overline{I}$.

Ahora supongamos que I es un ideal no primo de $R[x]$, entonces pueden ocurrir dos cosas:

1. *J no es primo en R.*
2. *J es primo en R pero $\overline{I}$ no es primo en $S[x]$. Por isomorfía con $R[x]/I$ que NO es dominio de integridad, en este caso tendremos que $S[x]/\overline{I}$ no es dominio de integridad luego $\overline{I}$ no es primo. $\overline{I}F[x]$ quizá sea primo pero en ese caso por Proposición 40.(3), $\overline{I}F[x] \cap S[x]$ será un ideal primo de $S[x]$ luego no será $\overline{I}$.*

■

Como F es un cuerpo, $F[x]$ será un dominio euclídeo y por extensión un dominio de ideales principales. Por tanto $\overline{I}F[x] = (h(x))$ será primo si y solo si $h(x)$ es un polinomio irreducible o nulo. Ahora solo necesitaremos una forma de comprobar que $\overline{I}$ es un ideal saturado, lo que veremos en la siguiente proposición.

Proposición 42. Sea S un dominio de integridad con cuerpo de fracciones F y sea A un ideal no nulo en $S[x]$. Supongamos que $AF[x] = (h(x))$ siendo $h(x)$ un polinomio de $S[x]$ con coeficiente director $a \in S$. Sea S_a la localización de S con respecto a las potencias de a. Entonces:

1. $AF[x] \cap S[x] = AS_a[x] \cap S[x]$
2. Si $\mathcal{A}$ denota el ideal generado por A y $1 - at$ en el anillo de polinomios $S[x, t]$, entonces $AS_a[x] \cap S[x] = \mathcal{A} \cap S[x]$

Combinando los resultados anteriores con la teoría de bases de Göbner llegamos al siguiente algoritmo.

Algoritmo para determinar si un ideal P de $k[x_1, x_2, \ldots, x_n]$ es primo

1. Calcular la base reducida de Gröbner de P, $G = \{g_1, g_2, \ldots, g_m\}$ respecto al orden monomial lexicográfico con $x_n > \cdots > x_1$.

Recordemos que la base reducida de Gröbner de cada $P_i = P \cap k[x_1, \ldots, x_i]$ será $G \cap k[x_1, \ldots, x_i] = \{g_1, \ldots, g_{m_i}\}$.

2. Determinar si P_1 es un ideal primo en $k[x_1]$ comprobando si $P_1 = 0$ o los generadores no nulos de P_1 son irreducibles en $k[x_1]$.

Ahora supongamos que para todo $j < i$ hemos comprobado que P_j es primo en $k[x_1, \ldots, x_j]$. Como hemos ido denotando hasta ahora $S = k[x_1, \ldots, x_{i-1}]/P_{i-1}$ y F es el cuerpo de fracciones de S.

En los pasos 3 y 4 comprobaremos las condiciones de la Proposición 41 para comprobar si el ideal P_i es primo, en caso negativo acabaremos el algoritmo determinando que P no es primo. En caso afirmativo repetiremos ambos pasos para P_{i+1}.

3. Si $m_i = m_{i-1}$ entonces P_i es claramente primo porque es el ideal nulo de $S[x_i]$. En caso contrario la imagen de P_i en $S[x_i]$ y $F[x_i]$ es un ideal no nulo generado por las imágenes de los elementos de su base de Göbner $\{g_1, \ldots, g_{m_i}\}$. Como $F[x_i]$ es un domino euclídeo podemos aplicar el algoritmo de euclides para encontrar un único elemento generador $h(x_i)$ en P_i cuya imagen en $F[x_i]$ genera toda la imagen de P_i en $F[x_i]$. Determinamos si $h(x_i)$ es irreducible en $F[x_i]$, en caso negativo P_i no es ideal primo y hemos acabado, en caso afirmativo pasamos al siguiente paso.
4. Sea $a \in k[x_1, \ldots, x_{i-1}]$ el coeficiente director de $h(x_i)$. Calcula la base reducida de Gröbner en $k[x_1, \ldots, x_i, t]$ del ideal generado por P_i y $1 - at$ respecto al orden monomial lexicográfico $t > x_i > \cdots > x_1$. Determinar si los elementos de esa base que también están en $k[x_1, \ldots, x_i]$ son $\{g_1, \ldots, g_{m_i}\}$. En caso afirmativo P_i es un ideal primo, en caso negativo P_i no es un ideal primo (y por tanto tampoco P).

Ejemplo:

Sea $P = (y^3 - xz, xy^2 - z^2, x^2 - yz)$ ideal de $\mathbb{Q}[x, y, z]$. Calculamos su base de Gröbner reducida respecto al orden monomial lexicografico dado por $x > y > z$ $G = \{x^2 - yz, xy^2 - z^2, xz - y^3, y^5 - z^3\}$.

Primero comprobamos si $P_1 = P \cap \mathbb{Q}[z]$ es primo, $G \cap \mathbb{Q}[z] = \emptyset$ luego $P_1 = (0)$ que es primo.

Ahora sabiendo que P_1 es primo comprobaremos que P_2 es primo. $P_2 = (y^5 - z^3)$, se puede probar que los ideales de la forma $(y^i - z^j)$ con i, j enteros positivos primos entre si siempre son primos. Finalmente comprobamos P. En este caso $S = \mathbb{Q}[y, z]/(y^5 - z^3)$ y F el cuerpo de fracciones de S:

$$S = \mathbb{Q}[\overline{z}] + \mathbb{Q}[\overline{z}]\overline{y} + \mathbb{Q}[\overline{z}]\overline{y}^2 + \mathbb{Q}[\overline{z}]\overline{y}^3 + \mathbb{Q}[\overline{z}]\overline{y}^4$$
$$F = \mathbb{Q}(\overline{z}) + \mathbb{Q}(\overline{z})\overline{y} + \mathbb{Q}(\overline{z})\overline{y}^2 + \mathbb{Q}(\overline{z})\overline{y}^3 + \mathbb{Q}(\overline{z})\overline{y}^4$$

Ya que $\overline{y}^5 = \overline{z}^3$. La imagen de P en $S[x]$ es el ideal $\overline{P}$ generado por los elementos $x^2 - \overline{yz}, x\overline{y}^2 - \overline{z}^2, x\overline{z} - \overline{y}^3, \overline{y}^5 - \overline{z}^3 = \overline{0}$. Aplicando el algoritmo de elucides en $F[x]$ llegamos a que la extensión de $\overline{P}$ en F está generada por $\overline{h}(x) = x - (\overline{yz}^5)/(\overline{y}^3\overline{z}^3)$ que es un elemento irreducible de $F[x]$ ya que tiene grado 1.

La imagen del polinomio $h(x) = xy^3z^3 - yz^5 \in P$ en $F[x]$ es $\overline{h}(x)$ luego genera la imagen de P en $F[x]$. Tomamos $a = y^3z^3$ para el paso (4) del algoritmo. Entonces lo que hay que hacer es calcular la base de Gröbner reducida del ideal $(x^2 - yz, xy^2 - z^2, xz - y^3, y^5 - z^3, 1 - y^3z^3t) \in \mathbb{Q}[t, x, y, z]$ respecto al orden monomial lexicografico $t > x > y > z$. Dicha base es $G' = \{ty^3z^3 - 1, tyz^5 - x, tz^6 - y^2, x^2 - yz, xy^2 - z^2, xz - y^3, y^5 - z^3\}$. Como $G' \cap \mathbb{Q}[x, y, z] = G$ podemos asegurar que P es un ideal primo.

4.3 Localización en módulos

Supongamos que M es un R-módulo y que D es un subconjunto cerrado por multiplicación de R que contiene a 1. Entonces podemos usar una construcción parecida a la de $D^{-1}R$ para construir un $D^{-1}R$-módulo $D^{-1}M$ a partir de M.

Cogemos el conjunto $M \times D$ y definimos una relación entre sus elementos:

$$(m_1, d_1) \sim (m_2, d_2) \quad \text{si y solo si } x(d_2m_1 - d_1m_2) = 0 \text{ para algún } x \in D$$

Esta resulta ser una relación de equivalencia. Denotemos la clase de equivalencia del elemento (m, d) por m/d y al conjunto de clases de equivalencia por $D^{-1}M$. Por último definimos las operaciones:

$$+ \colon D^{-1}M \times D^{-1}M \to D^{-1}M \qquad \frac{m_1}{d_1} + \frac{m_2}{d_2} = \frac{d_2m_1 + d_1m_2}{d_1d_2}$$

$$\bullet \colon D^{-1}R \times D^{-1}M \to D^{-1}M \qquad \left(\frac{r_1}{d_1}\right)\left(\frac{m}{d_2}\right) = \frac{rm}{d_1d_2}$$

Es fácil comprobar que estas operaciones están bien definidas y dan a $D^{-1}M$ estructura de $D^{-1}R$-módulo.

Definición. El $D^{-1}R$-módulo $D^{-1}M$ el el **modulo de fracciones** de M con respecto a D o la **localización** de M en D.

Notemos que al ser un $D^{-1}R$-módulo, $D^{-1}M$ es también un R-módulo, (basta coger $r/1 \in D^{-1}R$ en lugar de $r \in R$ en las operaciones anteriores), y existe un homomorfismo de R-módulos:

$$\pi\colon M \to D^{-1}M \qquad \text{donde } \pi(m) = \frac{m}{1}$$

De la definición de relación de equivalencia se sigue que:

$$ker\,\pi = \{m \in M \mid dm = 0 \text{ para algún } d \in D\}$$

Está aplicación es análoga a la que definimos para el Teorema 38 y de hecho comparte una propiedad universal análoga.

Sea N un R-módulo que cumple que la aplicación que surge de multiplicar cada elemento de N por $d \in D$ es biyectiva. En ese caso si $\psi\colon : M \to N$ es cualquier homomorfismo de R-módulos entre M y N, existe un único homomorfismo de R-módulos $\Psi\colon D^{-1}M \to N$ tal que $\Psi \circ \pi = \psi$.

Como R siempre es un R-módulo está definición es una generalización de la definición de localización en anillos que vimos al principio de la sección. Comprobemos que cuando R es un módulo de sí mismo las dos definiciones coinciden es trivial, porque en este caso todos los elementos que hemos definido son equivalentes.

Si M y N son R-módulos y $\varphi\colon M \to N$ es un homomorfismo de R-módulos entonces para todo subconjunto cerrado por productos D de R es fácil comprobar que hay inducido un homomorfismo de $D^{-1}R$-módulos de $D^{-1}M$ a $D^{-1}N$ definido por llevar m/d a $\varphi(m)/d$.

En general la localización de módulos es una operación muy "buena" en el sentido que se comporta bien con otras operaciones algebraicas tanto para anillos como para módulos.

Proposición 43. Sea R un anillo conmutativo y unitario, sea $D^{-1}R$ su localización respecto a un subconjunto D cerrado por productos que contiene a 1. Entonces:

1. La localización conmuta con la suma e intersección finita de ideales. Si I, J son ideales de R entonces:

   $$D^{-1}(I + J) = D^{-1}I + D^{-1}J \qquad D^{-1}(I \cap J) = D^{-1}I \cap D^{-1}J$$

   La localización también conmuta con cocientes:

   $$D^{-1}R/D^{-1}I = \overline{D}^{-1}(R/I)$$

   Donde $\overline{D}$ denota la imagen de D en el cociente (R/I).

2. La localización conmuta con la toma de radicales. Si I es un ideal de R entonces $rad(D^{-1}I) = D^{-1}rad\,I$. En concreto si N es el nilradical de R, entonces el nilradical de $D^{-1}R$ es $D^{-1}N$.

3. Ideales primarios corresponden con ideales primarios en la correspondencia de la Proposición 40(3). Si Q es un ideal P-primario de R con $D \cap Q = \emptyset$ entonces $D^{-1}P$ es un ideal primo y $D^{-1}Q$ es un ideal $D^{-1}P$-primario en $D^{-1}R$. Además se cumple que ${}^{c}(D^{-1}Q) = Q$.

4. La localización conmuta con la suma directa finita de módulos: Si M y N son R-módulos, entonces $D^{-1}(M \oplus N) \cong D^{-1}M \oplus D^{-1}N$.

5. La localización es exacta. Si:

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

Es una sucesión exacta corta de R-módulos. Es decir, L, M y N son R-módulos y $\psi\colon L \to M$ inyectiva, $\varphi\colon M \to N$ suprayectiva y $ker\,\varphi = \psi(L)$. Entonces esta sucesión induce una sucesión exacta corta de $D^{-1}R$-módulos:

$$0 \to D^{-1}L \xrightarrow{\psi'} D^{-1}M \xrightarrow{\varphi'} D^{-1}N \to 0$$

Demostración:

6. *Supongamos que* $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ *es una sucesión exacta corta de R-módulos.*

Todo elemento $D^{-1}N$ *es de la forma* n/d *con* $n \in N$ *y* $d \in D$. *Como* φ *es suprayectiva,* $n = \varphi(m)$ *para algún* $m \in M$, $\varphi'(m/d) = \varphi(m)/d = n/d$ *luego* $\varphi'\colon D^{-1}M \to D^{-1}N$ *es suprayectiva. Si* m/d *está en el núcleo de* φ' *entonces* $d_1\varphi(m) = 0$ *para algún* $d_1 \in D$. *Entonces* $\varphi(d_1 m) = 0$ *implica que* $d_1 m \in \psi(l)$ *para algún* $l \in L$ *por la exactitud de la sucesión original en* M. *Por tanto* $m/d = d_1 m/(d_1 d) = \psi(l)/(d_1 d) = \psi'(l/(d_1 d))$ *y* $ker(\varphi') \subseteq Im\,\psi'$. *Si* $\psi(l)/d \in Im\,\varphi'$, $\varphi'(\psi(l)/d) = \varphi(\psi(l))/d = 0$ *luego* $Im(\psi') \subseteq ker(\varphi')$ *y* $Im\,\psi' = ker\,\varphi'$ *lo que muestra la exactitud.*

Ahora solo queda ver que ψ' *es inyectiva. Supongamos que* $\psi'(l/d) = 0$ *entonces existe* d_2 *tal que* $d_2\psi(l) = 0$, $d_2 \in D$, *luego* $\psi(d_2 l) = 0$ *y como* ψ *es inyectiva* $d_2 l = 0$, *por tanto* $l/d = d_2 l/d_2 d = 0$ *luego* ψ' *es inyectiva. Por tanto:*

$$0 \to D^{-1}L \xrightarrow{\psi'} D^{-1}M \xrightarrow{\varphi} D^{-1}N \to 0$$

Es una sucesión exacta.

1. *Notemos que* $(i+j)/d = i/d + j/d$ *para* $i \in I, j \in J, d \in D$, *luego* $D^{-1}(I+J) \subseteq D^{-1}I + D^{-1}J$. *Al revés,* $i/d_1 + j/d_2 = (d_2 i + d_1 j)/(d_1 d_2)$ *par* $i \in I, j \in J$ *y* $d_1, d_2 \in D$, *luego* $d_2 i + d_1 j \in I + J$ *luego* $D^{-1}I + D^{-1}J \subseteq D^{-1}(I+J)$.

Para la intersección, $D^{-1}(I \cap J) \subseteq D^{-1}I \cap D^{-1}J$ *es inmediato. Sea* $a/d \in D^{-1}I \cap D^{-1}J$, *existe* d_1 *tal que* $d_1 a \in I$ *y* d_2 *tal que* $d_2 a \in J$, *luego* $d_1 d_2 a \in J \cap I$. *Por tanto* $a/d = d_1 d_2 a/d_1 d_2 d \in D^{-1}(I \cap J)$, *lo que por doble contenido implica* $D^{-1}I \cap D^{-1}J = D^{-1}(I \cap J)$.

Para los cocientes usamos (6). *Sea* ψ *la inclusión de* I *en* R *(que es inyectiva) y* φ *la proyección de* R *en* R/I *(que es suprayectiva). Es inmediato ver que forman una sucesión exacta corta:*

$$0 \to I \xrightarrow{\psi} R \xrightarrow{\varphi} R/I \to 0$$

Luego por (6) *tendremos la sucesión exacta:*

$$0 \to D^{-1}I \xrightarrow{\psi'} D^{-1}R \xrightarrow{\varphi'} \overline{D}^{-1}R/I$$

Donde $\psi'(D^{-1}I) = D^{-1}I = ker\,\varphi'$ *luego aplicando el primer teorema de isomorfía:*

$$D^{-1}R/D^{-1}I \cong \overline{D}^{-1}(R/I)$$

2. *Supongamos que* $a \in rad\, I$, *es decir* $a^n \in I$ *para* $n \geq 1$. *Entonces* $(a/d)^n = a^n/d^n \in D^{-1}I$, *luego* $D^{-1}rad\, I \subseteq rad(D^{-1}I)$. *Al revés, si* $a/d \in rad\,(D^{-1}I)$, *entonces* $a^n/d^n \in D^{-1}I$, *luego existe* d_1 *tal que* $d_1 a^n \in I$ *con* $d_1 \in D$. *Entonces* $(d_1 a)^n = d_1^{n-1}(d_1 a^n) \in I$, *lo que quiere decir que* $d_1 a \in rad\, I$ *y por último* $a/d = (d_1 a)/(d_1 d) \in D^{-1}(rad\, I)$. *Por tanto* $rad(D^{-1}I) \subseteq D^{-1}(rad\, I)$ *y por doble contenido* $rad(D^{-1}I) = D^{-1}(rad\, I)$.

3. *Notemos que* $D \cap P = \emptyset$ *equivale a que* $D \cap Q = \emptyset$, *ya que* $Q \subseteq P$ *y* D *es cerrado por productos luego si* $d \in D \cap P$ *tendremos que* $d^n \in D \cap Q$. *Vimos por Proposición* 40 *que si* P *es primo en* R *y* $D \cap P = \emptyset$ *entonces* $D^{-1}P$ *es primo en* $D^{-1}R$. *Ahora veamos que* $D^{-1}Q$ *es* $D^{-1}P$*-primario. Supongamos que* $(a/d_1)(b/d_2) \in D^{-1}Q$ *y* $a/d_1 \notin D^{-1}Q$, *luego* $a \notin Q$, *por tanto existe* $d \in D$ *tal que* $abd \in Q$, *como* $a \notin Q$, $d \notin Q$ *porque* $D \cap Q = \emptyset$ *tenemos que* $b \in rad\, Q = P$ *porque* Q *es* P*-primario. Entonces,* $b^n \in Q$ *y* $b^n/d_2^n \in D^{-1}Q$ *luego* $D^{-1}Q$ *es primario. En concreto, aplicando* (2) *sabemos que* $D^{-1}Q$ *es* $D^{-1}P$*-primario.*

Ahora supongamos que $D^{-1}Q = {}^eQ$ *un ideal* $D^{-1}P$*-primario.* ${}^c(D^{-1}Q) = {}^c({}^eQ) = \{r \in R \mid dr \in Q \text{ para algún } d \in D\}$, *pero como* $D \cap P = \emptyset$, $d \notin P$, *luego al ser* Q P*-primario si* $dr \in Q$ *y* $r \notin Q$ *tendremos que* $d \in P$ *que no ocurre porque* $P \cap D = \emptyset$. *Por tanto* $r \in Q$ *y al revés si* $r \in Q$ *evidentemente* $dr \in Q$ *luego* ${}^c(D^{-1}Q) = Q$.

4. *Es análoga a la de* (1).

5. *No la probaré. Es sencilla pero requiere adentrarse más en teoría de módulos.* ■

Fijándonos en la Proposición 40 vemos que localizar R respecto a un D nos ayuda a estudiar los ideales disjuntos de D ya que todos los demás se trivializan (sus extensiones son todo $D^{-1}R$). Esto puede verse al estudiar la el efecto de localizar en las descomposiciones primarias que vimos en la sección 2.

Proposición 44. Sea R un anillo noetheriano y sea:

$$I = Q_1 \cap \cdots \cap Q_m,$$

un ideal de R junto a una descomposición primaria mínima de dicho ideal, siendo cada Q_i un ideal P_i-primario. Supongamos D es un subconjunto de R que contiene a 1. Ordenamos los Q_i de manera que $D \cap P_i = \emptyset$ para $1 \leq i \leq t$ y $D \cap P_i \neq \emptyset$ para $t+1 \leq i \leq m$. En ese caso:

$$D^{-1}I = D^{-1}Q_1 \cap \cdots \cap D^{-1}Q_t$$

es una descomposición primaria mínima de $D^{-1}I$ en $D^{-1}R$ y cada $D^{-1}Q_i$ es $D^{-1}P_i$-primario. Es más, la contracción de $D^{-1}Q_i$ de vuelta a R es Q_i para $1 \leq i \leq t$ y:

$${}^c(D^{-1}I) = Q_1 \cap \cdots \cap Q_t$$

Demostración:

Por la Proposición 43 *vemos que efectivamente* $D^{-1}I = D^{-1}Q_1 \cap \cdots \cap D^{-1}Q_m$ *y que cada* $D^{-1}Q_i$ *es* $D^{-1}P_i$ *primario. Entonces usando la Proposición* 40.(2) *vemos que para* $Q_{t+1}, \ldots, Q_m$ *tendremos que* $D^{-1}Q_i = D^{-1}R$, *luego podemos simplificarlos de la intersección. Solo nos queda ver que la descomposición es mínima. Por la*

Proposición 40.(3) *si* $D^{-1}P_i = D^{-1}P_j$ *tendríamos que* $P_i = P_j$ *lo que no puede ocurrir porque la descomposición dada por* $Q_1, \ldots, Q_m$ *es mínima. Por la última afirmación de la Proposición* 43.(3) *si* $D^{-1}Q_i \supseteq \cap_{j\neq i} D^{-1}Q_j$ *tendremos al contraer de vuelta a* R *(recordar que la contracción es una preimagen)* $Q_i \supseteq \cap_{j\neq i} Q_j$ *lo cual es una contradicción.*

Usamos otra vez que la contracción es una preimagen y la Proposición 43.(3) *para comprobar que* ${}^c(D^{-1}I) = Q_1 \cap \cdots \cap Q_t$. ■

Este resultado nos permite probar la última afirmación del Teorema de Descomposición Primaria.

Corolario. Los ideales primarios Q_i que pertenecen a los primos aislados en una descomposición primaria mínima de un ideal I del anillo R están únicamente determinados por I.

Demostración:

Sea P *un primo aislado de* I. *Es decir,* P *es un elemento mínimo del conjunto de primos asociados a* I, $\{P_1, \ldots, P_n\}$. *Sea* $I = Q_1 \cap \cdots \cap Q_n$ *una descomposición primaria mínima de* I *en la que* Q_k *es el ideal* P*-primario. Localizamos respecto a* $D = R - P$. *Por la proposición anterior tendremos que* $D^{-1}I = D^{-1}Q_k$ *y* ${}^c(D^{-1}I) = Q_k$. *Como* ${}^c(D^{-1}I) = {}^c({}^eI) = \{r \in R \,|\, dr \in I \text{ para algún } d \in D\}$ *que no depende de la descomposición que hayamos elegido, solo de* I. *Por tanto* Q_k *está únicamente determinado.* ■

En la demostración del corolario anterior podemos ver la potencia de la localización. El efecto de localizar suele ser especialmente útil cuando localizamos respecto a un primo (como definimos en los ejemplos previos a la Proposición 40) como estudiaremos a continuación. La notación puede volverse un poco confusa, hay que tener claro que cuando nos refiramos a la localización $D^{-1}R$ del anillo R respecto a un ideal primo P siempre nos referimos a $D = R - P$ nunca a $D = P$. Denotaremos la localización de R con respecto al ideal primo P como R_P.

Definición. Un anillo conmutativo y unitario que tiene un único ideal maximal se denomina **anillo local**.

Proposición 45. Sea R un anillo conmutativo y unitario. Entonces las siguientes afirmaciones son equivalentes:

1. R es un anillo local con un ideal maximal M.
2. Si M es el conjunto de los elementos de R que no son unidades, entonces M es un ideal
3. Existe un ideal maximal M en R para el cual todo $1 + m$ con $m \in M$ es invertible en R.

Demostración:

$\underline{1 \to 2.}$ *Si* $a \in R$ *entonces* (a) *es* R *si y solo si* a *es invertible. En el caso de que* a *no sea invertible* (a) *será un ideal propio luego tendrá que estar contenido en el único ideal maximal* M, *por tanto* $a \in M$. *Obviamente si* a *es invertible* $a \notin M$ *ya que obligaría a que* $M = R$.

$\underline{2 \to 3.}$ *Supongamos que se cumple* (2) *con el ideal* M. *Sea* $m \in M$, *obviamente* $1 + m \notin M$ *porque en ese caso* $1 = 1 + m - m \in M$. *Como* $1 + m \notin M$, $1 + m$ *es invertible.* M *es maximal porque dado cualquier otro ideal propio* A *como los elementos de* A *no son unidades estarán en* M *luego* $A \subseteq M$

$\underline{3 \to 1.}$ *Supongamos que se cumple* (3) *con el ideal* M. *Cojamos* $a \in R$, $a \notin M$, *entonces* $(a) + M = R$ *(porque* M *es maximal), luego* $ab + M = 1$ *para algún* $b \in R$ *y* $m \in M$, *entonces tenemos que* $ab = 1 - m = 1 + (-m)$, *por la definición de* M a *es una unidad (*$(ab)c = 1$ *luego* $a(bc) = 1$*). Como todos los elementos no invertibles de* R *están en* M, M *contiene a todo el resto de ideales propios de* R *y por tanto es el único ideal maximal de* R. ∎

Proposición 46. Para cualquier anillo conmutativo R con 1, sea R_P la localización de R en un ideal primo P ($D = R - P$). Denotemos con ${}^eP$ la extensión de P a R_P.

1. R_P es un anillo local de ideal maximal ${}^eP$. La contracción de ${}^eP$ de vuelta a R es P y la aplicación π de R a R_P induce un una inyección del dominio de integridad R/P a $R_P/{}^eP$.

2. Si R es un dominio de integridad entonces también lo es R_P. En este caso el ideal maximal de R_P es PR_P donde identificamos P con su imagen dentro de R_P.

3. Los ideales primos en R_P están en correspondencia biyectiva con los ideales primos de R contenidos en P.

4. Si P es un ideal primo no nulo mínimo de R entonces R_P tiene un único ideal primo no nulo.

5. Si $P = M$ es un ideal maximal y I es cualquier ideal M-primario de R entonces $R_M/{}^eI \cong R/I$. En particular, $R_M/{}^eM \cong R/M$ y $({}^eM)/({}^eM)^n \cong M/M^n$.

Demostración:

$\underline{3.}$ *Si* P' *es un ideal primo de* R *entonces* $P' \cap (R - P) = \emptyset$ *si y solo si* $P' \in P$, *luego* (3) *es inmediato por Proposición* 40.(3).

$\underline{4.}$ *Consecuencia directa de* (3).

$\underline{1.}$ *Para la primera afirmación tenemos que* ${}^eP \neq R_P$ *por Proposición* 40.(2) *luego sale directamente de* (3).

Para la segunda sale fácilmente de Proposición 40.(2). ${}^c({}^eP) = \{r \in R \,|\, dr \in P \text{ para algún } d \in R - P\}$ *es inmediato ver que al ser* P *primo,* $dr \in R$ *con* $d \in R - P$ *ocurre si y solo si* $r \in R$.

Para la tercera afirmación. Es fácil ver que el núcleo de la aplicación que va de R *a* $R_P/{}^eP$ *(componer* π *con el cociente de* R_P *a* $R_P/{}^eP$*) es* ${}^c({}^eP) = \pi^{-1}({}^eP)$ *que es igual a* P. *Por tanto se induce una aplicación inyectiva de* R/P *a* $R_P/{}^eP$.

$\underline{2.}$ *Si* R *es un dominio de integridad entonces* $R - P$ *no tendrá divisores de* 0. *Como* R *es un dominio de integridad entonces* $R - P$ *no tiene divisores de* 0 *por lo que* R *se inyecta en* R_P *es por eso que* ${}^eP = PR_P$ *el ideal maximal de* R_P.

$\underline{5.}$ *Por la Proposición* 43.(1) *podemos pasar al cociente* R/I *para solo tener que estudiar el caso* $I = (0)$. *Con* $D = R - M$ *y* $\overline{D}$ *la imagen de* D *en* R/I*:*

$$R_M/{}^eI \cong \overline{D}^{-1}(R/I)$$

Luego si vemos que $\overline{D}^{-1}(R/I) \cong R/I$ *habríamos probado el resultado.*

$P = \overline{M}$ *la imagen de* M *en* R/I*, es el nilradical de* R/I*. Entonces* P *es la intersección de todos los ideales primos de* R/I *y maximal al mismo tiempo.* P *es el único ideal primo (y por tanto maximal) de* R/I*. Por la Proposición* 45 *todo elemento en* $R/I - P$ *es invertible luego con* $\overline{D} = (R/I) - P$ $D^{-1}(R/I) = (R/I)_P = R/I$*. Por tanto* $R_M/^e I \cong D^{-1}(R/I) = R/I$*. Lo demás son casos concretos como coger* $I = M$*.* ■

Definición. Sea M un R-módulo, sea P un ideal primo de R y sea $D = R - P$. El R_P-módulo $D^{-1}M$ recibe el nombre de **localización** de M en P, denotado M_P.

Localizar un modulo M en un primo P genera un nuevo modulo generalmente más sencillo. La idea es deducir propiedades de M a partir de propiedades de sus localizaciones M_P. La demostración del siguiente resultado nos da un ejemplo de como aplicaríamos dicha linea de razonamiento.

Proposición 47. Sea M un R-módulo. Entonces las siguientes afirmaciones son equivalentes:

1. $M = 0$.
2. $M_P = 0$ para todos los ideales primos P de R.
3. $M_{\mathfrak{m}} = 0$ para todos los ideales maximales $\mathfrak{m}$ de R.

Demostración:

$\underline{1 \to 2 \to 3}$ *Triviales.*

$\underline{3 \to 1}$ *Supongamos que* m *es un elemento no nulo de* M *y consideremos* $I = \{r \in R \mid rm = 0\}$ *que llamaremos aniquilador de* m*. Como* m *no nulo* I *será un ideal propio de* R*. Sea* $\mathfrak{m}$ *el ideal maximal de* R *que contiene a* I *y consideremos el elemento* $m/1$ *en la correspondiente localización* $M_{\mathfrak{m}}$ *de* $\mathfrak{m}$*. Como asumimos* (3) $m/1 = 0$*, pero eso quiere decir* $rm = r(m*1-0*1) = 0$ *para algún* $r \in R - \mathfrak{m}$*. Pero en ese caso* r *sería un elemento de* I *no contenido en* $\mathfrak{m}$*, una contradicción.* ■

No ocurre siempre que si todas las localizaciones de un modulo comparten una propiedad entonces dicho módulo también cumplirá la propiedad. Sin embargo, es algo que sucede a menudo y es una técnica que nos puede aportar una gran cantidad de información.

Otro ejemplo más importante sería el siguiente. Recordemos que R es un R-módulo y R_P puede verse como la localización del R-módulo R respecto a un ideal primo P de R.

Proposición 48. Sea R un dominio de integridad. Entonces R es la intersección de las distintas localizaciones de R: $R = \cap_P R_P$. Todavía más, $R = \cap_{\mathfrak{m}} R_{\mathfrak{m}}$ la intersección de todas las localizaciones de R respecto a ideales maximales.

Demostración:

Empezamos recordando que si R *es un dominio de integridad tendremos que cada localización de* R *es un subanillo del cuerpo de fracciones de* R *que contiene a* R*. Por tanto* $R \subseteq \cap_P R_P$*.*

Supongamos que a *es un elemento del cuerpo de fracciones de* R *que está contenido en* R_m *para todo ideal maximal* m *de* R*. Consideremos:*

$$I_a = \{d \in R \mid da \in R\}$$

Es fácil ver que I_a es un ideal de R y que $a \in R$ si y solo si $1 \in I_a$, es decir si $I_a = R$. Supongamos que $I_a \neq R$. Entonces hay un ideal maximal $\mathfrak{m} \subset R$ tal que $I_a \subset \mathfrak{m}$. Como $a \in R_\mathfrak{m}$ tendremos que $a = r/d$ para $r \in R$, $d \in R - \mathfrak{m}$, pero entonces $d \in I_a$ y $d \notin \mathfrak{m}$ lo que nos lleva a una contradicción. Por tanto $a \in R$, lo que quiere decir que $\cap_\mathfrak{m} R_\mathfrak{m} \subseteq = R$ y $R = \cap_\mathfrak{m} R_\mathfrak{m}$.

Ahora solo falta observar que si R es un dominio de integridad y A, B son ideales de R tales que $A \subseteq B$ entonces $R_B \subseteq R_A$. Por tanto como todo ideal primo de P de R tiene que estar contenido en algún ideal maximal $\mathfrak{m}$ y que cada ideal maximal $\mathfrak{m}$ de R es al mismo tiempo primo. Vemos que:

$$\bigcap_P R_P = \bigcap_\mathfrak{m} R_\mathfrak{m}$$

Lo que completa el resultado. ■

También tenemos el siguiente resultado:

Proposición 49. Sea R un dominio de integridad. Entonces las siguientes afirmaciones son equivalentes:

1. R es normal (R es íntegramente cerrada en su cuerpo de fracciones).
2. R_P es normal para todos los ideales primos P de R.
3. $R_\mathfrak{m}$ es normal para todos los ideales maximales $\mathfrak{m}$ de R.

Demostración:

Sea F el cuerpo de fracciones de R, como R es dominio de integridad las distintas localizaciones de R son subanillos de F.

$\underline{1 \to 2.}$ Supongamos que R es normal y que $y \in F$ es entero sobre R_P con P un ideal primo de R. Entonces y es raíz de un polinomio mónico en $R_P[x]$ de grado n y coeficientes a_i/d_i con $a_i \in R$, $d_i \notin P_i$. Tendremos que $y^n = y(d_0 d_1 \dots d_{n-1})$ es también raíz de un polinomio mónico de grado n en $R[x]$ resultante de multiplicar cada a_i/d_i por $(d_0 d_1 \dots d_{n-1})^{n-i}$. Como R es cerrado por enteros vemos que $y' \in R$ luego $y = y'/(d_0 d_1 \dots d_{n-1}) \in R_P$ luego R_P también es cerrado por enteros lo que nos da (2).

$\underline{2 \to 3}$ Es trivial porque todos los ideales maximales son primos.

$\underline{3 \to 1}$ Supongamos ahora que $R_\mathfrak{m}$ es normal para todos los ideales maximales m de R y sea y un elemento de F entero sobre R. Como $R \subseteq R_\mathfrak{m}$ para todo $\mathfrak{m}$ y tambien será integral sobre cada $R_\mathfrak{m}$ y al ser estos cerrados por enteros $y \in \cap_\mathfrak{m} R_\mathfrak{m}$. Por la Proposición 48 *tenemos que $y \in R$ lo que prueba el resultado.* ■

4.4 Anillos locales de Variedades afines algebraicas

Para lo que queda del capítulo k denotará un cuerpo algebraicamente cerrado y V una variedad afín sobre ese cuerpo con anillo de coordenadas $k[V]$.

Cuando V es una variedad afín $k[V]$ es un dominio de integridad luego tiene cuerpo de fracciones:

$$k(V) = \{f/g \mid f, g \in k[V], g \neq 0\}$$

Los elementos de $k(V)$ reciben el nombre de **funciones racionales** en V y $k(V)$ es el **cuerpo de funciones racionales** de V. Recordar que por la construcción del cuerpo de fracciones, $f_1/g_1 = f_2/g_2$ cuando $g_2 f_1 = g_1 f_2$.

Definición. Decimos que f/g es **regular** en un punto $v \in V$ si existe algún $f_1, g_1 \in k[V]$ con $f/g = f_1/g_1$ y $g_1(v) \neq 0$.

En un cuerpo k la división está definida para cualquier denominador que no sea 0. Por tanto, que f/g sea regular en v quiere decir que f/g es equivalente a una tupla f_1/g_1 para la cual $f_1(v)/g_1(v)$ está bien definido en k, es decir, f/g tiene un valor bien definido al evaluarse en v. f_1/g_1 no tiene porque ser única, pero de existir otra tupla f_2/g_2 válida tendríamos que $f_1/g_1 = f_2/g_2$, es decir $g_2 f_1 = g_1 f_2$ luego $g_2(v)f_1(v) = g_1(v)f_2(v)$ y $f_1(v)/g_1(v) = f_2(v)/g_2(v)$. Por tanto el valor de f/g en v es el mismo si f/g es regular en v.

Ejemplo:

> La variedad $V = \mathcal{Z}(xz - yw)$ en $\mathbb{A}^4$ tiene un anillo de coordenadas $k[V] = k[x, y, z, w]/(xz - yw)$. Consideramos el elemento $f = \overline{x}/\overline{y}$ en el anillo cociente $k(V)$. Como $\overline{x}\overline{z} = \overline{y}\overline{w}$ en $k[V]$ entonces f también se puedes escribir como $\overline{w}/\overline{z}$. De $f = \overline{x}/\overline{y}$ vemos que f es regular en todos los puntos de V donde $\overline{y} \neq 0$, de $f = \overline{w}/\overline{z}$ vemos que f es regular en todos los puntos de V donde $\overline{z} \neq 0$.

Si $f/g \in k(V)$ es regular en un punto v es porque $f/g = f_1/g_1$ con $g_1(v) \neq 0$, entonces claramente f/g será regular también en el entorno abierto $\mathcal{Z}(g_1)^c$ de v en la topología de Zariski de V. Como todo conjunto abierto de la topología de Zariski de una variedad, es denso en la topología de dicha variedad. Tenemos que toda función racional de V tiene valor bien definido en un conjunto denso (en "casi todo punto").

Definición. Para cada punto $v \in V$ el conjunto de funciones racionales en V que son regulares en v:

$$\mathcal{O}_{v,V} = \{f/g \in k(V) \mid f/g \text{ regular en } v\}$$

recibe el nombre de **anillo local** de V en v.

Observemos que una función racional f/g es regular en v si y solo si $f/g = f_1/g_1$ con $g_1 \notin \mathcal{I}(v)$. Esto es lo mismo que decir $\mathcal{O}_{v,V}$ es la localización de $k[V]$ respecto al ideal maximal (y por tanto primo) $\mathcal{I}(v)$. Como vimos en la Proposición 46(1) $k[V]_{\mathcal{I}(v)} = \mathcal{O}_{v,V}$, el anillo local de V en v es efectivamente un anillo local. El único ideal maximal será:

$$\mathfrak{m}_{v,V} = \{f/g \in \mathcal{O}_{v,V} \mid f/g = f_1/g_1, f_1(v) = 0, g_1(v) \neq 0\}$$

Está expresión se obtiene de Proposición 45(2) teniendo en cuenta que todos los elementos $f/g \in \mathcal{O}_{v,V}$ para los cuales $f(v) \neq 0$ es decir $f \notin \mathcal{I}(V)$ son invertibles porque f es un denominador válido.

Otras observaciones:

- $\mathcal{O}_{v,V}$ es un dominio de integridad por Proposición 46(2).
- $\mathcal{O}_{v,V}/\mathfrak{m}_{v,V} \cong k[V]/\mathcal{I}(v) \cong k$ por Proposición 46(6).

Proposición 50. Si V es una variedad afín sobre un cuerpo algebraicamente cerrado k entonces las funciones racionales de V regulares en todos los puntos de V son precisamente las funciones polinómicas de $k[V]$.

Demostración:

Los $\mathcal{I}(v)$ con v un punto de V son los ideales maximales de $k[V]$ por el teorema de ceros de Hilbert. Aplicando el Proposición 48 se prueba el resultado. ■

Sea $\varphi\colon V \to W$ un morfismo entre variedades afines con homomorfismo de k-álgebras asociado $\widetilde{\varphi}\colon k[W] \to k[V]$. Si para $v \in V$ tenemos que $\varphi(v) = w \in W$ entonces sabemos que $\widetilde{\varphi}(\mathcal{I}(w)) = \mathcal{I}(v)$. Por tanto $\widetilde{\varphi}$ induce un homomorfismo entre anillos locales:

$$\widetilde{\varphi}\colon \mathcal{O}_{w,W} \to \mathcal{O}_{v,V} \text{ definido por } \widetilde{\varphi}(h/k) = \widetilde{\varphi}(h)/\widetilde{\varphi}(k)$$

también es fácil comprobar que $\widetilde{\varphi}^{-1}(\mathfrak{m}_{v,V}) = \mathfrak{m}_{w,W}$. Sea $f/g \in \mathfrak{m}_{v,V}$, tendremos que existe $f_1/g_1 = f/g$ con $f_1(v) = 0$ ($f_1(v) \in \mathcal{I}(v)$), $g_1(v) \neq 0$. Entonces como $\widetilde{\varphi}^{-1}(\mathcal{I}(V))$ es un ideal de $k[W]$ que contiene a $\mathcal{I}(w)$ (que es maximal) tendremos que $\widetilde{\varphi}^{-1}(\mathcal{I}(V)) = \mathcal{I}(w)$. Por tanto $\forall g \in \widetilde{\varphi}^{-1}(f)(w)$, $g(w) = 0$ y a partir de ahí es fácil ver que $\widetilde{\varphi}^{-1}(\mathfrak{m}_{v,V}) = \mathfrak{m}_{w,W}$. Los homomorfismos de anillos locales que cumplen esta propiedad reciben el nombre de homomorfismos locales.

El anillo local $\mathcal{O}_{v,V}$ puede usarse para dar una definición algebraica de "suave" (en el sentido de existencia de derivada) de el conjunto V en el punto v. Supongamos que $V = \mathcal{Z}(f)$ es un hiperplano en $\mathbb{A}^n$ definido por los ceros del polinomio irreducible $f \in k[x_1, \ldots, x_n]$. Para cualquier punto $v = (v_1, \ldots, v_n) \in V$ definimos $D_v(f)(x_1, \ldots, x_n)$ como el polinomio lineal:

$$D_v(f)(x_1, \ldots, x_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(v) x_i$$

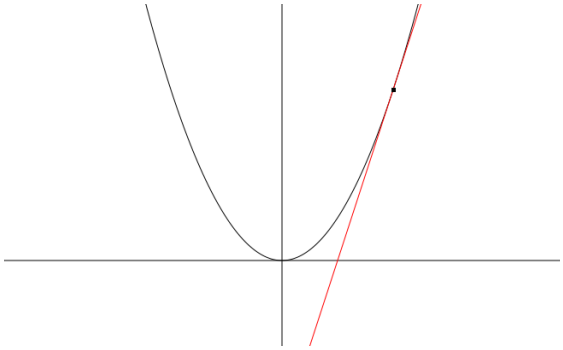
Tomando las derivadas parciales de la forma usual ($ax_i^n \to nax_i^{n-1}$). Si definimos $\mathbf{T}$ como la variedad lineal (conjunto de soluciones de un sistema de ecuaciones lineales) $\mathcal{Z}(D_v(f)(x_1, \ldots, x_n))$, entonces la traslación $v + \mathbf{T}$ es "tangente" a $\mathcal{Z}(f)$ en v. Además observemos que $D_v(f)(x_1 - v_1, \ldots, x_n - vn)$ será el desarrollo de Taylor de grado 1 de f en v.

Ejemplo:

Supongamos que $f = x^2 - y \in k[x, y]$, de tal forma que $V = \mathcal{Z}(f)$ es simplemente la parábola $y = x^2$. Derivamos $\partial f/\partial x = 2x$ y $\partial f/\partial y = -1$, que en $v = (2, 4)$ valen 4 y -1 respectivamente, entonces:

$$D_{(2,4)}(f)(x, y) = 4x - y$$

y la variedad lineal correspondiente $\mathbf{T}$ es la recta $y = 4x$. Ahora cogemos $(2, 4) + \mathbf{T}$ que es la recta tangente a la parábola en el punto $(2, 4)$:



Definición. Definimos como **espacio tangente** a V en v a la variedad lineal:

$$\mathbb{T}_{v,V} = \mathcal{Z}(\{D_v(f)(x_1, \ldots, x_n) \mid f \in \mathcal{I}(V)\})$$

Como las derivadas parciales son k-lineales y obedecen a la regla del producto usual para las derivadas podemos calcular el espacio tangente a partir de los generadores de $\mathcal{I}(V)$

$$\text{Si} \quad \mathcal{I}(V) = (f_1, \ldots, f_m) \quad \text{entonces} \quad \mathbb{T}_{v,V} = \bigcap_{i=1}^{m} \mathcal{Z}(D_v(f_i))$$

Proposición 51. Sea V una variedad algebraica sobre un cuerpo algebraicamente cerrado k y sea v un punto de V con anillo local $\mathcal{O}_{v,V}$ con correspondiente anillo maximal $\mathfrak{m}_{v,V}$. Entonces existe un isomorfismo de k-espacios vectoriales:

$$(\mathbb{T}_{v,V})^* \cong \mathfrak{m}_{v,V}/\mathfrak{m}_{v,V}^2$$

donde $(\mathbb{T}_{v,V})^*$ denota el espacio vectorial dual a $\mathbb{T}_{v,V}$.

Demostración:

Sea $(k^n)^*$ el espacion dual a k^n. Como cada $D_v(f)$ es una función lineal, tenemos que D_v es una transformación linear de $k[x_1, \ldots, x_n]$ a $(k^n)^*$ ($f \to D_v(f)$).

Sea M_v el ideal maximal en $k[x_1, \ldots, x_n]$ generado por el conjunto $(x_1 - v_1, \ldots, x_n - v_n)$ es el ideal de funciones que se anulan en v. El cociente $M_v/\mathcal{I}(V)$ de M_v en $k[V]$ es el ideal $\mathcal{I}(v)$ de funciones en V que se anulan en v, además $\mathcal{I}(v)^2 = M_v^2 + \mathcal{I}(v)$. $\mathcal{O}_{v,V}$ es la localización de $k[V]$ respecto a $\mathcal{I}(v)$, identificando $\mathcal{I}(v)$ con su imagen en $\mathcal{O}_{v,V}$ tenemos $\mathfrak{m}_{v,V} = \mathcal{I}(v)\mathcal{O}_{v,V}$ por la Proposición 46.(2).

Por definición de D_v tenemos que $D_v(x_i - v_i) = x_i$ y como estas derivadas forman una base de $(k^n)^*$, sigue que la imagen de M_v por D_v es todo $(k^n)^*$ (las imagenes de los generadores de M_v generan $(k^n)^*$).

El kernel de D_v está formado por aquellos elementos de $k[x_1, \ldots, x_n]$ cuyo desarrollo de Taylor en v comienza como poco en el grado 2. Estos son los elementos de M_v^2. Por tanto tenemos el isomorfismo:

$$D_v \colon M_v/M_v^2 \longrightarrow (k^n)^*$$

El espacio tangente $\mathbb{T}_{v,V}$ es un subespacio de k^n, luego toda función lineal en k^n puede restringirse a una función lineal en $\mathbb{T}_{v,V}$. Componiendo D_v con esta restricción da una transformación lineal:

$$D \colon M_v \xrightarrow{D_v} (k^n)^* \xrightarrow{rest} (\mathbb{T}_{v,V})^*$$

además dicha transformación es suprayectiva (por ser composición de dos transformaciones suprayectivas). Ya hemos visto que $\mathcal{I}(v)^2 = M_v^2 + \mathcal{I}(V)$, *luego* $\mathcal{I}(v)/\mathcal{I}(v)^2 \cong M_v/(M_v^2 + \mathcal{I}(V))$. *Por la Proposición* 46.(5) *obtenemos* $\mathfrak{m}_{v,V}/\mathfrak{m}_{v,V}^2 \cong \mathcal{I}(v)/\mathcal{I}(v)^2$.

Para completar la demostración basta mostrar que $\ker D = M_v^2 + \mathcal{I}(V)$ *ya que en ese caso:*

$$\mathfrak{m}_{v,V}/\mathfrak{m}_{v,V}^2 \cong M_v/(M_v^2 + \mathcal{I}(V)) = M_v/\ker D \cong (\mathbb{T}_{v,V})^*$$

Un polinomio f *está en* $\ker D$ *si y solo si* $D_v(f)$ *es nulo en* $\mathbb{T}_{v,V}$, *es decir, si y solo si el término lineal del polinomio de Taylor de* f *en* v *está en* $\mathcal{I}(\mathbb{T}_{v,V})$. *Como los términos lineales de las funciones en* $\mathcal{I}(V)$ *generan* $\mathcal{I}(\mathbb{T}_{v,V})$ *sigue que* $f \in \ker D$ *si y solo si* $f - g$ *tiene como término lineal* 0 *para algún* g *en* $\mathcal{I}(V)$. *Pero esto es equivalente a* $f \in \mathcal{I}(V)M_v^2$ *completando la demostración.* ■

Definición. Si V es una variedad algebraica, la **dimensión** de V, denotada $dim\, V$, está definida como el grado de transcendencia del cuerpo de funciones racionales $k(V)$ sobre el cuerpo k.

Nota: El grado de transcendencia de un cuerpo sobre un subcuerpo es una manera de medir la parte que no es algebraica de dicha extensión. El grado de transcendencia de F/K es el cardinal del mayor conjunto de F algebraicamente independiente sobre K.

Como cada anillo local $\mathcal{O}_{v,V}$ tiene a $k(V)$ como su cuerpo de fracciones, la dimensión de V sobre k puede calcularse a partir del grado de transcendencia sobre k del cuerpo de fracciones de cualquiera de sus anillos locales.

Definición. Decimos que V es **no singular** en un punto $v \in V$ (o que v es un punto no singular de V) si la dimensión del k-espacio vectorial $\mathbb{T}_{v,V}$ es $dim\, V$. Equivalentemente (por la proposición anterior), si $dim_k(\mathfrak{m}_{v,V}/\mathfrak{m}_{v,V}^2) = dim\, V$. En caso contrario v será un punto **singular** de V. Si ningún punto es singular se dice que V es **suave**.

La interpretación geométrica de esto sería lo siguiente, si V es no singular en un punto v, por v hay tantas tangentes a V como sea posible.

Para ver si una variedad V es no singular en un punto v miraremos si $dim_k(\mathfrak{m}_{v,V}/\mathfrak{m}_{v,V}^2) = dim\, \mathcal{O}_{v,V}$.

Si $f_1, \ldots, f_m$ son generadores de $\mathcal{I}(V)$ con $V \subseteq \mathbb{A}^n$ con V una variedad algebraica, entonces la dimensión de V se calcula a partir de una base de Gröbner de $\mathcal{I}(V)$. Para determinar la dimensión de $\mathbb{T}_{v,V}$ vemos que es un espacio vectorial solución de un sistema de m ecuaciones lineales con n incógnitas (los $D_v(f_i)(x_1, \ldots, x_n) = 0$). Si r es el rango de la matriz $m \times n$ que define este sistema, $r_{i,j} = \partial f_i/\partial x_j(v)$, entonces $\mathbb{T}_{v,V}$ es un espacio vectorial de dimensión $n - r$. A partir de aquí se puede probar lo siguiente:

1. $dim\, V \leq dim_k(\mathbb{T}_{v,V}) \leq n$ para todo $v \in V \subseteq \mathbb{A}^n$
2. El conjunto de puntos singulares de V es un conjunto cerrado en la topología de Zariski de V distinto de V. Por tanto el conjunto de puntos no singulares es abierto, esto implica que es denso en V (todos los abiertos son densos en la topología de Zariski de V).

Además hay otro resultado que daremos sin demostración y que relaciona todavía más las propiedad de la geometría local de V y sus anillos locales.

3. Si v es un punto no singular de V, entonces $\mathcal{O}_{v,V}$ es un dominio de factorización única. En concreto $\mathcal{O}_{v,V}$ es íntegramente cerrado.

La variedad V se dice **factorial** si $\mathcal{O}_{v,V}$ es un dominio de factorización única para todo $v \in V$, y **normal** si $\mathcal{O}_{v,V}$ es íntegramente cerrado para cada $v \in V$. Esto junto con el (3) anterior da:

$$\text{variedades suaves} \subseteq \text{variedades factoriales} \subseteq \text{variedades normales}$$

5 El espectro primo de un anillo

A lo largo de esta sección todos los anillos serán por regla general conmutativos y unitarios.

Está sección busca dar un nuevo enfoque a toda la teoría anterior. Hasta ahora solíamos empezar con un concepto geométrico sobre conjuntos algebraicos afines para después buscarles análogos en la teoría de anillos. Por ejemplo, en la sección 1 introducíamos los morfismos entre conjuntos algebraicos y después veíamos que estos morfismos inducían (y eran inducidos) por homomorfismos de anillos entre sus anillos de coordenadas. Ahora sin embargo, la pregunta será, si tenemos un anillo cualquiera R. ¿Podríamos definir una geometría a partir de él? La respuesta es sí, es más, este nuevo enfoque nos ayuda a aplicar conceptos de geometría algebraica que ya hemos visto a situaciones mucho más generales, no solamente k-álgebras y conjuntos algebraicos afines.

En el siguiente párrafo es una introducción al tipo de razonamiento que vamos a utilizar en está sección y no pretende ser demasiado riguroso. Sin embargo si nos puede dar una visión general de los que vamos a explicar a continuación.

Tengamos pues un anillo conmutativo y unitario R que haga el papel de $k[V]$. ¿Cuales serían los elementos de su 'V' correspondiente? Una primera aproximación sería coger los ideales maximales de R porque por el teorema de ceros de Hilbert los puntos de V estaban en correspondencia biyectiva con los ideales maximales de $k[V]$ (siempre que k fuese algebraicamente cerrado). Desafortunadamente esta aproximación tiene un gran problema. Si $\widetilde{\varphi}\colon R' \to R$ es un homomorfismo de anillos entonces querriamos que $\widetilde{\varphi}^{-1}(M)$ con M ideal maximal de R fuese un ideal maximal de R' (para que una aplicación entre objetos algebraicos induzca una aplicación entre objetos geométricos), sin embargo la preimagen de un ideal maximal no tiene por qué ser un ideal maximal. Esto es algo que sí que cumplen los ideales primos.

Definición. Sea R un anillo conmutativo y unitario. El **espectro primo** de R, denotado $Spec\, R$, es el conjunto de todos los ideales primos de R. Por su parte el conjuto de todos los ideales maximales de R se denomina **espectro maximal** de R, $mSpec\, R$.

Ejemplo:

> Si $R = \mathbb{Z}$ entonces $Spec\, R$ consiste en el ideal (0) y todos los ideales de la forma (p) con p un entero primo. En este caso $mSpec\, R$ serán todos los elementos de $Spec\, R$ a excepción de (0).

Volvamos a la analogía con $k[V]$ y V cuando k es algebraicamente cerrado. Evaluar los elementos de $k[V]$ en un punto de $v \in V$ nos da un homomorfismo suprayectivo de $k[V]$ a k con núcleo $\mathcal{I}(v)$, por tanto $k[V]/\mathcal{I}(v) \cong k$, en este isomorfismo $f(v)$ es análogo a $\overline{f} \in k[V]/\mathcal{I}(v)$.

Definición. Si $f \in R$ entonces el **valor** de f evaluado en el punto $P \in Spec\, R$, $f(P)$, es el elemento $\overline{f} \in R/P$.

Observemos que las evaluaciones de f en los distintos puntos $P \in Spec\, R$ pueden estar en distintos dominios de integridad. Todavía más, un elemento f no está únicamente determinado por los valores que toma al ser evaluado. Sin embargo si f, g tienen el mismo valor en cada punto de $Spec\, R$ esto quiere decir que $f - g$ está contenido en

la intersección de todos los ideales primos de R, esto equivale a decir que $f - g$ está contenido en el nilradical de R.

Ahora con una definición para evaluación podemos ponernos a definir los análogos $\mathcal{Z}$ e $\mathcal{I}$ en este contexto. Sea $A \subseteq R$:

$$\mathcal{Z}(A) = \{P \in X \mid A \subseteq P\} \subseteq Spec\, R$$

Elegimos está definición porque si $f \in A$ y $P \in \mathcal{Z}(A)$, entonces $f \in P$ luego $f(P) = \overline{f} \in R/P = \overline{0}$. $\mathcal{Z}(A)$ es el conjunto de puntos de $Spec\, R$ donde se anulan todos los elementos de A. Además es inmediato que si $I = (A)$ el ideal generado por A en R entonces $\mathcal{Z}(A) = \mathcal{Z}(I)$ luego no perdemos elementos si nos limitamos a evaluar $\mathcal{Z}$ en ideales.

Sea $Y \subseteq Spec\, R$, definimos

$$\mathcal{I}(Y) = \bigcap_{P \in Y} P$$

La intersección de todos los ideales primos de Y. Igual que antes si $P \in Y$ y $f \in \mathcal{I}(Y)$ entonces $f \in P$ luego $f(P) = \overline{0} \in R/P$.

Proposición 52. Sea R un anillo conmutativo y unitario. Entonces las aplicaciones $\mathcal{Z}$ e $\mathcal{I}$ entre R y $Spec\, R$ satisfacen:

1. Para todo ideal I de R, $\mathcal{Z}(I) = \mathcal{Z}(rad(I)) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$ y $\mathcal{I}(\mathcal{Z}(I)) = rad\, I$.
2. Para cualquier par de ideales I, J de R, $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.
3. Si $\{I_j\}$ es una colección arbitraria de ideales de R entonces $\mathcal{Z}(\cup I_j) = \cap \mathcal{Z}(I_j)$,

Podemos ver en está proposición que para está nueva definición $\mathcal{Z}$ vuelve a definir una topología a través de sus cerrados:

$$\mathcal{T} = \{\mathcal{Z}(I) \,|\, I \text{ es un ideal de } R\}$$

Definición. La topología de $Spec\, R$ que tiene como cerrados a los $\mathcal{Z}(I)$ con I un ideal de R recibe el nombre de **topología de Zariski** de $Spec\, R$.

En la topología de Zariski de $Spec\, R$ la clausura de Zariski de un conjunto unipuntual $\{P\}$ consiste en todos los ideales primos de R que contienen a P. En particular, un punto es cerrado por si mismo en la topología de Zariski si y solo si es un ideal maximal.

Definición. Los ideales maximales de R se denominan **puntos cerrados** de $Spec\, R$.

Un conjunto cerrado V de la topología de Zariski es irreducible si no es la unión no trivial de dos conjuntos de cerrados. Esto es lo mismo que decir que todo conjunto abierto de su topología de subespacio es denso. Además un conjunto cerrado de $Spec\, R$, $Y = \mathcal{Z}(I)$ es irreducible si y solo si $\mathcal{I}(Y) = rad\, I$ es primo.

Sea $Y = \mathcal{Z}(I)$, primero supongamos que I es reducible es decir $Y = Y_1 \cup Y_2$ con $Y_1 = \mathcal{Z}(I_1), Y_2 = \mathcal{Z}(I_2)$ cerrados distintos de $Spec\, R$. Como $Y_1 \neq Y$ existirá $f_1 \in R$ tal que $f_1 \in \mathcal{I}(Y_1) - \mathcal{I}(Y)$. Del mismo modo podemos encontrar $f_2 \in \mathcal{I}(Y_2) - \mathcal{I}(Y)$. Tenemos que $Y = \mathcal{Z}(I) = Y_1 \cup Y_2 = \mathcal{Z}(I_1) \cup \mathcal{Z}(I_2) = \mathcal{Z}(I_1 I_2)$, por tanto $\mathcal{I}(Y) = rad\, I = rad(I_1 I_2)$, $f_1 f_2 \in rad\, I_1 rad\, I_2$ y es fácil ver que $f_1 f_2 \in rad(I_1 I_2) = \mathcal{I}(Y)$. Por tanto

$\mathcal{I}(Y)$ no es primo. Para la inversa supongamos que $\mathcal{I}(Y)$ no es primo, entonces existe $f_1, f_2 \notin \mathcal{I}(Y)$ para los cuales $f_1 f_2 \in \mathcal{I}(Y)$. Sean $Y_1 = \mathcal{Z}(f_1) \cap Y$ y $Y_2 = \mathcal{Z}(f_2) \cap Y$. $Y_1, Y_2 \neq Y$ ya que en caso contrario tendríamos que $f_1 \in \mathcal{I}(Y_1) = \mathcal{I}(Y)$ lo que es una contradicción (análogo para Y_2). Por último vemos que $Y \subseteq \mathcal{Z}(f_1 f_2) = \mathcal{Z}(f_1) \cup \mathcal{Z}(f_2)$, luego $Y_1 \cup Y_2 = Y$, es decir, Y no es irreducible.

Proposición 53. La aplicaciones $\mathcal{Z}$ e $\mathcal{I}$ definen dos biyecciones inversas entre si:

Conjuntos cerrados en la topología de Zariski de $Spec\, R$	$\xrightarrow{\mathcal{I}}$ $\xleftarrow[\mathcal{Z}]{}$	Ideales radicales de R

Además bajo esta correspondencia los puntos cerrados de $Spec\, R$ corresponden a los ideales maximales de R y los conjuntos irreducibles de $Spec\, R$ corresponden a los ideales primos de R.

Sobre un cuerpo algebraicamente cerrado k un homomorfismo entre dos k-álgebras $\varphi\colon R \to S$ cumple que la preimagen de un ideal maximal de S es un ideal maximal de R. Cuando R es el anillo de coordenadas de un conjunto algebraico afín V, tenemos que $Spec\, R$ no contienes solo a los puntos de V (como los puntos cerrados de $Spec\, R$, $mSpec\, R$) sino también puntos que se corresponden con todas las subvariedades de V (como los puntos no cerrados de $Spec\, R$ todos los primos no maximales) luego $Spec\, R$ no es exactamente una generalización de los conjuntos algebraicos. Lo que si hemos conseguido como veremos a continuación es que cada homorfismo de anillos entre los objetos algebraicos R, S induzca una aplicación continua respecto a las topologías de Zariski de los objetos geométricos $Spec\, R, Spec\, S$ tal y como ocurría con los morfismos.

Sea $\varphi\colon R \to S$ un homomorfismo entre dos anillos conmutativos y unitarios tal que $\varphi(1_R) = 1_S$. En ese caso si P es un primo de S, $\varphi^{-1}(P)$ es un ideal primo de R, luego φ induce una aplicación $\varphi^*\colon Spec\, S \to Spec\, R$ con $\varphi^*(P) = \varphi^{-1}(P)$.

Proposición 54. Todo homomorfismo entre dos anillos conmutativos y unitarios R, S $\varphi\colon R \to S$ para el cual $\varphi(1_R) = \varphi(1_S)$ induce una aplicación $\varphi^*\colon Spec\, S \to Spec\, R$ continua respecto a las topologías de Zariski de $Spec\, S$, $Spec\, R$.

Demostración:

Que φ^* existe ya lo hemos visto luego ya solo queda ver que efectivamente φ^* es continua.

Sea $\mathcal{Z}(I) \subseteq Spec\, R$ un conjunto cerrado en la topología de Zariski de $Spec\, R$. $\varphi^{*-1}(\mathcal{Z}(I))$ son los elementos de $Spec(S)$ tales que $I \subseteq \varphi^{-1}(P)$. Pero para $P \in Spec\, S$ $I \subseteq \varphi^{-1}(P)$ si y solo si $\varphi(I) \subseteq P$, lo que equivale a $\varphi(I)S \subseteq P$, luego $\varphi^{*-1}(\mathcal{Z}(I)) = \mathcal{Z}(\varphi(I)S)$, que es cerrado en $Spec\, S$. Por tanto φ^* es continua respecto a las topologías de Zariski. ∎

Con esto ya hemos generalizado los conjuntos algebraicos V que solo teníamos definidos en k-álgebras finitamente generadas como $k[x_1, \ldots, x_n]$ a $Spec\, R$ que existe en cualquier anillo R. No es exactamente una generalización como ya hemos visto pero conserva la gran mayoría de las propiedades.

Ya hemos definido un análogo a las variedades algebraicas dentro $Spec\, R$ (los cerrados irreducibles en la topología de Zariski), luego podemos empezar a plantearnos como definir un análogo para el cuerpo de funciones racionales.

Recordemos: cuando V es una variedad afín algebraica de un cuerpo algebraicamente cerrado k.

- $k(V)$ el cuerpo de funciones racionales de V, es el cuerpo de fracciones de $k[V]$. Cada elemento de $\alpha \in k(V)$ se representa a partir de tuplas a/f con $a, f \in k[V]$, cada representación no tiene por qué ser única.
- α es regular en un punto $v \in V$ si existe algún representante de α, a/f, tal que $f(v) \neq 0$ de manera que a/f de un valor bien definido para α en v. Además a/f no solo define α en v sino en todos los demás puntos p donde $f(p) \neq 0$, el conjunto de dichos p (denotado V_f) es un conjunto abierto de la topología de Zariski de V.
- Un solo representante a/f no basta para definir α en todos los puntos que es regular, pero la unión de los V_f de todos los representantes forma un cubrimiento del conjunto de puntos en el que α es regular (porque siempre tiene que haber al menos un representate para cada punto).

Estás son las características de las funciones racionales que buscamos generalizar.

Definición. Para cada $f \in R$ denotemos por X_f al conjunto de ideales primos en $Spec\, R$ que no contienen a f. Esto equivale a los puntos de $Spec\, R$ en los que f no se anula. Decimos que X_f es un **conjunto abierto principal** en $Spec\, R$.

Claramente como X_f es $\mathcal{Z}(f)^c$ será un conjunto abierto en la topología de Zariski de $Spec\, R$.

Proposición 55. Sea $f \in R$ y sea $X_f \subseteq X = Spec\, R$ el correspondiente conjunto abierto principal.

1. $X_f = X$ si y solo si f es una unidad, $X_f = \emptyset$ si y solo si f es nilpotente
2. $X_f \cap X_g = X_{fg}$
3. $X_f \subseteq X_{g_1} \cup \cdots \cup X_{g_n}$ si y solo si $f \in rad(g_1, \ldots, g_n)$, en particular $X_f = X_g$ si y solo si $rad(f) = rad(g)$
4. Los conjuntos abiertos principales forman una base de la topologia de Zariski de $Spec\, R$
5. La aplicación natural $r \to r/1$ entre R y R_f induce un homeomorfismo de $Spec\, R_f$ a X_f, siendo R_f la localización de R en f.
6. El espectro primo de cualquier anillo es compacto.
7. Si $\varphi\colon R \to S$ es un homomorfismo de anillos con $\varphi(1_R) = \varphi(1_S)$ entonces para la aplicación inducida $\varphi^*\colon Y = Spec\, S \to X = Spec\, R$ tenemos que $\varphi^{*-1}(X_f) = Y_{\varphi(f)}$.

Demostración:

1, 2 *y* 7 *son sencillos a si que no los probare aquí.*

3. $X_{g_1} \cup \cdots \cup X_{g_n}$ *está formado por los ideales primos* P *que NO contienen a todos los* g_i. *Por tanto* $X_{g_1} \cup \cdots \cup X_{g_n}$ *es el complementario del conjunto cerrado* $\mathcal{Z}((g_1, \ldots, g_n))$ *que consiste en los ideales primos* P *que contienen al ideal generado*

por $g_1, \ldots, g_n$. Si $(g_1, \ldots, g_n) = R$ entonces $X_{g_1} \cup \cdots \cup X_{g_n} = X$ y no hay nada que probar. En caso contrario tendremos que $X_f \subseteq X_{g_1} \cup \cdots \cup X_{g_n}$ si y solo todo primo P tal que $f \notin P$ también satisface que $P \notin \mathcal{Z}((g_1, \ldots, g_n))$. Esto equivale a decir que f está contenido en la intersección de todos los ideales primos que contienen a $(g_1, \ldots, g_n)$, $rad((g_1, \ldots, g_n))$.

4. Si $U = X - \mathcal{Z}(I)$ conjunto abierto de X, entonces U es la unión de todos los conjuntos X_f con $f \in I$

5. El homomorfismo de anillos de R a la localización R_f

$$\begin{array}{rccc} \pi\colon & R & \to & R_f \\ & r & \to & r/1 \end{array}$$

establece una biyección entre ideales primos de R que no contienen a f y los ideales primos de R_f (por Proposición 40.(3)). La correspondiente aplicación Zariski continua π^* de $Spec\, R_f$ a $Spec\, R$ es por consiguiente biyectiva. Como todo ideal en R_f es extensión de algún ideal en R (Proposición 40.(1)), sigue que la aplicación inversa a π^* también es continua, lo que prueba 5.

6. Todo conjunto abierto es unión de conjuntos abierto principales por 4 luego basta probar que si X está cubierto por abiertos principales X_{g_i} (i en un conjunto de índices $\mathcal{J}$) entonces X es unión finita de algunos g_i. Si el ideal generado por los g_i fuese propio en R, entonces I estaría contenido en algún ideal maximal P. Pero en este caso el elemento P en $X = Spec\, R$ no estaría cubierto por los X_{g_i}. Por tanto $I = R$ luego $1 \in R$ puede ser escrito como combinación lineal finita $1 = a_1 g_{i_1} + \cdots + a_n g_{i_k}$ con $i_1, \ldots, i_k \in \mathcal{J}$. Consideremos la unión finita $X_{g_{i_1}} \cup \cdots \cup X_{g_{i_n}}$. Cualquier punto P en X no contenido en esta unión es un ideal propio primo en R conteniendo $g_{i_1}, \ldots, g_{i_k}$ y por tanto a 1 lo cual es una contradicción. Por tanto $X = X_{g_{i_1}} \cup \cdots \cup X_{g_{i_k}}$ un subcubrimiento finito de X. ∎

Ahora definiremos un análogo del cuerpo de funciones racionales de una variedad V para $X = Spec\, R$.

Vimos que en una variedad V, una función racional $\alpha \in k(V)$ es regular en algún conjunto U abierto de V. En cada punto de $v \in U$ existe algún representante a/f de α para el cual $f(v) \neq 0$, este a/f también representa un elemento de $\mathcal{O}_{v,V} = k[V]_{\mathcal{I}(v)}$. De este modo podemos ver α como una función de U a la unión disjunta de localizaciones $\mathcal{O}_{v,V}$ con $v \in U$, a cada punto de U se le asigna al elemento representado por a/f en $\mathcal{O}_{v,V}$. Además vimos que podemos usar el representante a/f no solo para v sino para todo punto en un entorno abierto V_f de v.

Estos razonamientos pueden sonar extraños cuando V una variedad ya que $k[V]$ es un dominio de integridad luego los $\mathcal{O}_{v,V}$ son subanillos de $k(V)$, y por tanto a/f es un representante del mismo elemento ya sea en $k(V)$ o en cualquier otro $\mathcal{O}_{v,V}$ con $f \in \mathcal{I}(v)$. Sin embargo, ahora ya no estamos trabajando con dominios de integridad por lo que es importante recalcar la diferencia entre a/f como representante de un elemento de $k(V)$ o a/f como representante de un elemento de $\mathcal{O}_{v,V}$.

Definición. Supongamos que U es un subconjunto Zariski abierto de $Spec\, R$. Si $U = \emptyset$, definimos $\mathcal{O}(U) = 0$. En cualquier otro caso definiremos $\mathcal{O}(U)$ como el conjunto de funciones $s\colon U \to \bigsqcup_{Q \in U} R_Q$ de U a la unión disjunta de localizaciones R_Q para cada primo $Q \in U$ que cumplen las siguientes dos propiedades:

1. $s(Q) \in R_Q$ para cada $Q \in U$

2. Para cada $P \in U$ existe un entorno abierto $X_f \subseteq U$ de P en U y un elemento a/f^n en la localización de R_f definiendo s en X_f. Es decir, $s(Q) = a/f^n \in R_Q$ para cada $Q \in X_f$.

Dado $Q_1, Q_2 \in X_f$, $a/f^n \in R_{Q_1}$, $a/f^n \in R_{Q_2}$ no son el mismo elemento, R_{Q_1}, R_{Q_2} ni siquiera tienen por qué compartir elementos, lo que comparten es el representante común para ambas clases de equivalencia. Y puesto que una clase de equivalencia puede tener varios representantes, es perfectamente posible que dos $a/f^n, b/g^m$ definan a $s(Q)$ al mismo tiempo en los $Q \in U \cap (X_f \cap X_g)$, solo necesitamos que a/f^n, b/g^m sean representantes del mismo elemento en cada R_Q.

Algunas observaciones:

- Se puede demostrar que si s, t son elementos de $\mathcal{O}(U)$ entonces $s + t$ y st son también elementos de $\mathcal{O}(U)$, luego $\mathcal{O}(U)$ es un anillo.
- Si U' es un subconjunto abierto de U, entonces la aplicación que surge de restringir los elementos de $\mathcal{O}(U)$ a elementos de $\mathcal{O}(U')$ es un homomorfismo de anillos.

Definición. Sea R un anillo conmutativo y unitario y sea $X = Spec\, R$.

- La colección de todos los anillos $\mathcal{O}(U)$ para los abiertos de la topología de Zariski de X junto a las restricciones $\mathcal{O}(U) \to \mathcal{O}(U')$ para $U' \subseteq U$ recibe el nombre de **haz de estructura** de X, denotada $\mathcal{O}_X$ (o $\mathcal{O}$ si no da lugar a confusión).
- Cada elemento $s \in \mathcal{O}(U)$ recibe el nombre de **sección** de $\mathcal{O}$ sobre U. Los elementos de $\mathcal{O}(X)$ reciben el nombre de **secciones globales** de $\mathcal{O}$.

El siguiente resultado generaliza la Proposición 50 que nos dice que la únicas funciones racionales de una variedad V regulares en todo punto son los elementos de $k[V]$.

Proposición 56. Sea $X = Spec\, R$ y sea $\mathcal{O}$ su haz de estructura. Las secciones globales de $\mathcal{O}$ son los elementos de R. Es decir, $\mathcal{O}(X) \cong R$. De hecho, si X_f es un abierto principal en X de algún $f \in R$ se cumple que $\mathcal{O}(X_f) \cong R_f$.

Demostración:

Supongamos que $a/f^n \in R_Q$ para $Q \in X_f$ determina un elemento en $\mathcal{O}(X_f)$, es inmediato que la aplicación resultante $\psi\colon R_f \to \mathcal{O}(X_f)$ es un homomorfismo de anillos. Supongamos que $a/f^n = b/f^m$ en R_Q para todo $Q \in X_f$, es decir para cada $Q \in X_f$ existe $g \in R - Q$ para la que $g(af^m - bf^n) = 0$ en R. Si I es el ideal en R de elementos $r \in R$ con $r(af^m - bf^n) = 0$, ahora como cada g está en I sabemos que I no está contenido en Q para ningún $Q \in X_f$. Dicho de otra forma todo ideal primo de R que contiene a I también contiene a f (no está en X_f). Por tanto f estará contenido en la intersección de todos los ideales primos que contienen a I o lo que es lo mismo $f \in rad\, I$. Por la definición de $rad\, I$ tenemos que $f^N \in I$ para algún entero positivo N luego $f^N(af^m - bf^n) = 0$. Esto demuestra que $a/f^n = b/f^m$ en R_f luego ψ es inyectivo.

Supongamos ahora que $s \in \mathcal{O}(X_f)$. Entonces por definición, X_f puede ser cubierto por abiertos principales X_{g_i} en los que $s(Q) = a_i/g_i^{n_i} \in R_Q$ para cada $Q \in X_{g_i}$. Por Proposición 55.(6) podemos tomar un cubrimiento finito de g_i y después eligiendo bien los a_i podemos asumir que todos los n_i son iguales a n el maximo de todos ellos ($a_i/g_i^{n_i} = (a_i g_i^{n-n_i})/g_i^n$). Como $s(Q) = a_i/g_i^n = a_j/g_j^n$ en R_Q para todo

$Q \in X_{g_ig_j} = X_{g_i} \cap X_{g_j}$, la inyectividad de ψ (definido sobre $R_{g_ig_j}$ muestra que $a_i/g_i^n = a_j/g_j^n$ en $R_{g_ig_j}$ es decir, existe un entero positivo N tal que $(g_ig_j)^N(a_ig_j^n - a_jg_i^n) = 0$ o lo que es lo mismo:

$$a_ig_i^n g_j^{n+N} = a_ig_i^{n+N}g_j^N$$

Podemos asumir que tomado N los suficientemente grande N servirá para todo par i, j. Como X_f es la unión de los $X_{g_i} = X_{g_i^{n+N}}$, por Proposición 55.(3) tendremos que $f \in rad(g_1^n, \ldots, g_k^n)$. Entonces:

$$f^M = \sum_i b_i g_i^{n+N}$$

para algún entero positivo M y $b_i \in R$. Definimos $a = \sum b_I a_i g_i^N \in R$ entonces

$$g_j^N a_j f^M = \sum b_i(a_j g_i^{n+N} g_j^N) = \sum b_i(a_i g_i^N g_j^{n+N}) = g_j^{n+N} a$$

Sigue que $a/f^M = a/g_j^n$ en R_{g_j} y que los elementos en $\mathcal{O}(X_f)$ definidos por a/f^m en R_f coincide con X_{g_j}, luego en todo X_f puesto que estos abiertos principales cubren todo X_f. Por tanto la aplicación ψ da un isomorfismo $R_f \cong \mathcal{O}(X_f)$. Tomando $f = 1$ obtenemos $R \cong \mathcal{O}(x)$. ∎

En el caso de variedades afines V, el anillo local $\mathcal{O}_{v,V}$ en el punto $v \in V$ es la unión de todos los anillos de funciones regulares en conjuntos U, para los conjuntos abiertos U que contienen a v, teniendo lugar está unión dentro de $k(V)$. Desafortunadamente para $X = Spec\, R$ ya no tenemos un anillo tan conveniente donde realizar la unión. Busquemos otra manera de construir $\mathcal{O}_{P,X}$. Con $P \in X$. Empezamos cogiendo las parejas (s, U) con U un conjunto abierto de X que contenga al punto P y $s \in \mathcal{O}(U)$. Identificaremos dos pares $(s, U) \sim (s', U')$ si existe un conjunto abierto $U'' \subseteq U \cap U'$ para el que la restricción s y s' a U'' es el mismo elemento de $\mathcal{O}(U'')$. El conjunto de clases de equivalencia se denomina **limite directo** del anillo $\mathcal{O}(U)$, denotado $\varinjlim \mathcal{O}(U)$.

Definición. Si $P \in X = Spec\, R$ y sea $\mathcal{O}$ su haz de estructura, entonces el limite directo $\varinjlim \mathcal{O}(U)$, de los anillos $\mathcal{O}(U)$ para los abiertos $U \subseteq X$ que contienen a P se denomina **tallo** de su haz de estructura en P, denotado $\mathcal{O}_{X,P}$ (o sencillamente $\mathcal{O}_P$ si no da lugar a confusión).

Comprobemos que $\mathcal{O}_P$ con $P \in X$ es un anillo. Sean (s_1, U_1), (j_1, V_1) y sean s_1' y j_1' las restricciones de s_1, j_1 a $U_1 \cap V_1$ (la unión finita de abiertos es finita). Como $\mathcal{O}(U_1 \cap V_1)$ es un anillo luego podemos sumar y multiplicar s_1' y j_1'. Entonces definimos $(s_1, U_1) + (j_1, V_1) = (s_1' + j_1', U_1 \cap V_1)$ y $(s_1, U_1) * (j_1, V_1) = (s_1'j_1', U_1 \cap V_1)$. Veamos que estas operaciones están bien definidas para $\mathcal{O}_P$, sean $(s_2, U_2) \sim (s_1, U_1)$ y $(j_2, V_2) \sim (j_1, V_1)$. Existe U, V abiertos donde las restricciones de $(s_1, U_1), (s_2, U_2)$ y $(j_1, V_1), (j_2, V_2)$ a U, V respectivamente coinciden. Es fácil ver que $s_1 + j_1, s_2 + j_2$ y s_1j_1, s_2j_2 coincidirán en $U \cap V$ luego ambas operaciones están bien definidas. También es fácil que estas operaciones dan a $\mathcal{O}_P$ estructura de anillo.

Proposición 57. Sea $X = Spec\, R$ y sea $\mathcal{O}$ su haz de estructura. Entonces su tallo en el punto $P \in X$, $\mathcal{O}_{P,X}$, es isomorfo a la localización de R en P, R_P.

Demostración:

Si (s,U) representa un elemento en el tallo $\mathcal{O}_P$, entonces $s(P)$ es un elemento de la localización R_P. Por la definición de limite directo este elemento no depende de la elección del representante (s,U), por tanto este proceso nos da un homomorfismo de anillos bien definido $\varphi\colon \mathcal{O}_P \to R_P$. Si $a, f \in R$ con $f \notin P$, entonces la aplicación $s(Q) = a/f \in R_Q$ define un elemento de $\mathcal{O}(X_f)$. Entonces la clase de equivalencia de (s, X_f) en el tallo $\mathcal{O}_\mathcal{P}$ va a a/f en R_P por φ, luego φ es suprayectiva. Para ver que φ es además inyectiva, supongamos que las clases de (s,U) y (s',U') en $\mathcal{O}_P$ satisfacen $s(P) = s'(P)$ en R_P. Por definición de $\mathcal{O}(U)$, $s = a/g^n$ en X_g para algún $g \notin P$. De manera similar $s' = b/(g')^m$ en $X_{g'}$ para algún $g' \notin P$. Como $a/g^n = b/g'^m$ en R_P, existe algún $h \notin P$ para el que $h(a(g')^m - bg^n) = 0$ en R. Si $Q \in X_{gg'h} = X_g \cap X_{g'} \cap X_h$ esta última igualdad muestra que $a/g^n = b/g'^m$ en R_Q es decir, s y s' coinciden cuando ser restringen a $X_g g' h$. Por definición del limite directo, (s,U) y (s,U') definen el mismo elemento en el tallo $\mathcal{O}_P$, lo que prueba que φ es inyectivo y acaba de probar la proposición. ∎

Notemos que la proposición anterior implica que $\mathcal{O}_{X,P}$ es un anillo local.

Por la proposición anterior la localización R_P para $P \in Spec\, R$ es análoga al anillo $\mathcal{O}_{v,V}$ de funciones regulares en una variedad V. Si $\mathfrak{m}_P$ denota el ideal maximal $PR_P \in R_P$ y $k(P) = R_P/\mathfrak{m}_P$ denota el correspondiente anillo de fracciones (que por la proposición Proposición 46(1) es también el cuerpo de fracciones de R/P), entonces el **espacio tangente** lo definimos como el $k(P)$-espacio vectorial dual a $\mathfrak{m}_P/\mathfrak{m}_P^2$. Observemos que está definición viene inspirada por la Proposición 51.

Definición. Sea R un anillo conmutativo y unitario. El par $(Spec\, R, \mathcal{O}_{Spec\, R})$ del espacio $Spec\, R$ junto a su haz de estructura recibe el nombre de **esquema afín**.

El esquema afín nos da una generalización completamente algebraica de la geometría de conjuntos algebraicos afines que podemos aplicar a cualquier anillo algebraico.

A continuación estudiaremos relaciones entre los esquemas afines de dos anillos R y S cuando existe un homomorfismo de anillos entre ambos.

Supongamos que tenemos el homomorfismo de anillos $\varphi\colon R \to S$. Por la Proposición 55(7) sabemos que existe una aplicación continua inducida por φ, $\varphi^*\colon Y = Spec\, S \to X = Spec\, R$ y que para dicha aplicación $(\varphi^*)^{-1}(X_f) = Y_{\varphi(g)}$. Por tanto podemos encontrar una aplicación inducida entre las correspondientes secciones de las haces de estructura:

Sea $Q' \in Y$ un punto de $Spec\, S$ y sea $Q = \varphi^*(Q') = \varphi^{-1}(Q') \in X$ su punto correspondiente en $Spec\, R$. Cogemos $U \subseteq X$ abierto de X que contenga a Q, $U' = (\varphi^*)^{-1}(U)$ que será un abierto de Y que contendrá a Q'. φ además induce un homomorfismo de anillos de R_Q a $S_{Q'}$ definido por $\varphi_Q(a/f) = \varphi(a)/\varphi(f) \in S_{Q'}$ para $f \notin Q$. Sea $s \in \mathcal{O}_X(U)$ una sección del haz de estructura de X correspondiente a U definida en un entorno X_g de P como a/g^n. Entonces la composición:

$$\begin{array}{rccccccc} s'\colon & U' & \xrightarrow{\varphi^*} & U & \xrightarrow{s} & \bigsqcup_{Q\in U} R_Q & \xrightarrow{\varphi_Q} & \bigsqcup_{Q'\in U} S_{Q'} \\ & Q' & \longrightarrow & Q & \longrightarrow & s(Q) & \longrightarrow & \varphi_Q(s(Q)) \end{array}$$

define una aplicación definida en el entorno $Y_{\varphi(g)}$ por $\varphi(a)/\varphi(g)^n$ luego $s' \in \mathcal{O}_Y(U')$. Es fácil comprobar que la aplicación resultante $\varphi^\#\colon \mathcal{O}_X(U) \to \mathcal{O}_Y(U')$ es un homo-

morfismo de anillos compatible con la restricción de aplicaciones en $\mathcal{O}_X, \mathcal{O}_Y$. Por tanto $\varphi^\#$ inducirá un homomorfismo de anillos $\varphi^\#\colon \mathcal{O}_{X,P} \to \mathcal{O}_{Y,P'}$ para cualquier punto $P' \in Spec\, S$ y su punto correspondiente $P = \varphi^*(P') \in Spec\, R$. Basta coger $\varphi^\#(s,U) = (\varphi^\#(s), U')$, como $\varphi^\#$ es compatible con la restricción tendremos que el homomorfismo estará bien definido. Además, aplicando la Proposición 57 el homomorfismo $\varphi^\#$ va de $\mathcal{O}_{X,P} \cong R_P$ a $\mathcal{O}_{Y,P'} \cong S'_P$ y es el homomorfismo natural φ_P entre localizaciones inducido por φ. En particular, la preimagen por $\varphi^\#$ del ideal maximal del anillo local $\mathcal{O}_{Y,P'}$ es el ideal maximal del anillo local $\mathcal{O}_{X,P}$.

Definición. Sean R y S dos anillos conmutativos y unitarios. Cojamos entonces $(Spec\, R, \mathcal{O}_{Spec\, R})$ y $(Spec\, S, \mathcal{O}_{Spec\, S})$ sus esquemas afines. Un **morfismo entre esquemas afines** de $(Spec\, S, \mathcal{O}_{Spec\, S})$ a $(Spec\, R, \mathcal{O}_{Spec\, R})$ es un par $(\varphi^*, \varphi^\#)$ tal que:

1. $\varphi^*\colon Spec\, S \to Spec\, R$ es una aplicación continua respecto a las topologías de Zariski de S y R.
2. Existe un homomorfismo de anillos $\varphi^\#\colon \mathcal{O}(U) \to \mathcal{O}(\varphi^{*-1}(U))$ para cada conjunto abierto U en la topología de Zariski de $Spec\, R$, $\varphi^\#$ es conmutativa con la restricción de aplicaciones.
3. Si $P' \in Spec\, S$ con punto correspondiente $P = \varphi^*(P') \in Spec\, R$, entonces la preimagen del ideal maximal de $\mathcal{O}_{Spec\, S, P'}$ por $\varphi^\#\colon \mathcal{O}_{Spec\, R, P} \to \mathcal{O}_{Spec\, S, P'}$ es el ideal maximal de $\mathcal{O}_{Spec\, R, P}$.

En está definición $\varphi^\#$ no es una función en concreto sino una familia de homomorfismos de anillos que van desde anillos $\mathcal{O}_{Spec\, S}(U)$ con U un abierto de $Spec\, S$ a $\mathcal{O}_{Spec\, R}(\varphi^*(U))$.

Ya hemos visto que un morfismo $\varphi\colon R \to S$ induce un homomorfismo de esquemas afines de $(Spec\, S, \mathcal{O}_{Spec\, S})$ a $(Spec\, R, \mathcal{O}_{Spec\, R})$.

Al revés, supongamos que $(\varphi^*, \varphi^\#)$ es un morfismo de esquemas afines de $(Spec\, S, \mathcal{O}_{Spec\, S})$ a $(Spec\, R, \mathcal{O}_{Spec\, R})$. En el caso particular $U = Spec\, R$, $(\varphi^*)^{-1}(U) = Spec\, S$ tenemos por la segunda propiedad de estos morfismos que existe un homomorfismo de anillos $\varphi^\#\colon \mathcal{O}_{Spec\, R}(Spec\, R) \to \mathcal{O}_{Spec\, S}(Spec\, S)$. Por la Proposición 56 sabemos que $\mathcal{O}_{Spec\, R}(Spec\, R) \cong R$ y $\mathcal{O}_{Spec\, S}(Spec\, S) \cong S$ como anillos. Componiendo estos dos isomorfismos con $\varphi^\#$ vemos que $\varphi^\#$ induce un homomorfismo de anillos $\varphi\colon R \to S$.

Por la Proposición 57 y por la compatibilidad con la restricción de homomorfismo de la propiedad (2) tenemos que $\varphi, \varphi^\#$ respetan el siguiente diagrama.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & & \downarrow \\ R_P & \xrightarrow{\varphi^\#} & S_{P'} \end{array}$$

Donde las flechas verticales representan la localización de los anillos R y S ($\pi(r) = r/1$). Por la propiedad (3) de $\varphi^\#$ tenemos que $(\varphi^\#)^{-1}(P'S_{P'}) = PR_P$, de lo que deducimos que $\varphi(P') = P$. Luego la aplicación entre $Spec\, S$ y $Spec\, R$ inducida por φ es precisamente φ^*. Que φ induce $\varphi^\#$ es fácil a partir de ahí.

Teorema 58. Todo homomorfismo de anillos conmutativos y unitarios $\varphi\colon R \to S$ induce un morfismo entre esquemas afines:

$$(\varphi^*, \varphi^\#)\colon (Spec\, S, \mathcal{O}_{Spec\, S} \to (Spec\, R, \mathcal{O}_{Spec\, R})$$

Además cada morfismo entre esquemas afines es inducido por algún homomorfismo de anillos φ.

Este teorema es análogo al Teorema 9.

Anexo: teoría de módulos

En este anexo haré una brevisima introducción a la teoría de módulos que se utiliza en este trabajo.

Definición. Sea R un anillo (no necesariamente conmutativo ni unitario). Un **R-módulo a izquierda** o **módulo a izquierda** sobre R es un conjunto M con:

1. Una operación binaria $+$ entre elementos de M para la que M es grupo abeliano
2. Una acción de R sobre M (aplicación $R \times M \to M$), que para elementos $r \in R$, $m \in M$ denotaremos por rm. Está acción cumple las siguientes propiedades:
   (a) $(r_1 + r_2)m = r_1m + r_2m$ para todo $r_1, r_2 \in R$, $m \in M$
   (b) $(r_1r_2)m = r(sm)$ para todo $r_1, r_2 \in R$, $m \in M$
   (c) $r(m_1 + m_2) = rm_1 + rm_2$ para todo $r \in R$, $m \in M$

   En el caso en el que R sea unitario exigimos una nueva propiedad

   (d) $1m = m$ para todo $m \in M$

Análogamente a los módulos a izquierda se pueden definir los módulos a derecha. Si nos referimos a módulo nos referiremos por defecto a módulo a izquierda. Los espacios vectoriales son los módulos en el caso concreto de que R sea un cuerpo.

Definición. Sea R un anillo y sea M un R-módulo. Un R-submódulo es un subgrupo N de M cerrado por la acción de R sobre M, $rn \in N$ para todo $r \in R$, $n \in N$

Observemos que todo anillo R es un R-módulo y que todo ideal I de R es un R-submódulo de R.

Definición. Sea R un anillo y M, N R-módulos.

- Una aplicación $\varphi\colon : M \to N$ es un **homomorfismo de R-módulos** si cumple
  1. $\varphi(x + y) = \varphi(x) + \varphi(y)$, para todo $x, y \in M$.
  2. $\varphi(rx) = r\varphi(x)$, para todo $r \in R$, $x \in M$.
- Un homomorfismo de R-módulos es un **isomorfismo** si es biyectivo. M y N se dicen **isomorfos**, denotado $M \cong N$, si existe un isomorfismo de R-módulos entre ellos.
- Sea $\varphi\colon M \to N$ un homomorfismo de R-módulos.
  - $ker\,\varphi = \{m \in M \mid \varphi(m) = 0\}$ es el **núcleo** de φ.
  - $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ para algún } m \in M\}$ es la **imagen** de M por φ.

Como M un "R-módulo" es un grupo más una operación con R podemos definir el grupo cociente respecto a un submódulo I como haríamos en un grupo cualquiera. M/I seguirá siendo un R-módulo.
Los homomorfismos de módulos cumplen los cuatro teoremas de isomorfía.

Teorema. 1. *(Primer teorema de isomorfía)* Sean M, N R-módulos y sea $\varphi\colon M \to N$ un homomorfismo de R-módulos. Entonces $ker\,\varphi$ es un submódulo de M y $M/ker\,\varphi \cong \varphi(M)$.

2. *(Segundo teorema de isomorfía)* Sean A, B submódulos del R-módulo M. Entonces $(A+B)/B \cong A/(A \cap B)$.

3. *(Tercer teorema de isomorfía)* Sea M un R-módulo, sean A y B submódulos de M con $A \subseteq B$. Entonces $(M/A)/(B/A) \cong M/B$.

4. *(Cuarto teorema de isomorfía)* Sea N un submódulo del R-módulo M. Existe una biyección entre los submódulos de M que contienen a N y los submódulos de M/N. La correspondencia viene dada por $A \leftrightarrow A/N$. Además está correspondencia conmuta con sumas e intersecciones, $A+B \leftrightarrow A/N+B/N$, $A \cap B \leftrightarrow (A/N \cap B/N)$.

La demostración es muy sencilla usando los teoremas de isomorfía para grupos.

Definición. Sea M un R-módulo, sea N un submódulo de M ($N = M$ es posible). N está finitamente generado como N-módulo por $\{n_1, \ldots, n_s\} \subseteq M$ si todos los elementos de N se pueden expresar de la forma:

$$r_1 n_1 + r_2 n_2 + \cdots + r_s n_s$$

Con $r_1, r_2, \ldots, r_s \in R$.

Definición. Sea $X_1, \ldots, X_n$ una secuencia (también puede ser infinita) de R-módulos y sean $\varphi_i\colon X_i \to X_{i+1}$ homomorfismos de R-módulos. Entonces

$$X_1 \xrightarrow{\varphi_1} X_2 \xrightarrow{\varphi_2} \ldots$$

es una **sucesión** de homomorfismos de R-módulos. En concreto si para cada i

$$Im\,\varphi_i = ker\,\varphi_{i+1}$$

diremos que se trata de una **sucesión exacta**.

Sean A, B, C R-módulos la sucesión:

$$0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$$

es exacta si y solo si ψ es inyectiva, φ es suprayectiva y $Im\,\psi = ker\,\varphi$. Esta estructura recibe el nombre de **sucesión exacta corta**.

Conclusión

Durante todo este trabajo hemos visto que el álgebra puede ser una potente herramienta para abordar problemas de naturaleza geométrica. Es más, la geometría algebraica nos brinda todo un nuevo punto de vista para estudiar las soluciones de sistemas de ecuaciones a un nivel más conceptual. Es un buen ejemplo de que en las matemáticas nada existe en un vacío, no debemos pensar en la geometría, cálculo, álgebra etc, como si se tratasen de compartimentos estancos porque en muchos casos la mejor manera de avanzar en un campo es utilizando herramientas propias de otro campo totalmente distinto.

References

[1] David S. Dummit y Richard M.Foote *Abstract Algebra*. John Wiley & Sons, Inc. 2004.

[2] Buchberger's Algorithm,
`http://www.lpthe.jussieu.fr/~talon/buchberger.html`

[3] Geometría algebraica.
`https://es.wikipedia.org/wiki/Geometra_algebraica`

[4] Algebraic geometry.
`en.wikipedia.org/wiki/Algebraic_geometry`

[5] Rowland, Todd. "Algebraic Geometry." From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein.
`https://mathworld.wolfram.com/AlgebraicGeometry.html`